DG-LB1054

5 Port Load Sharing Router

User Manual

V1.0

2013-11-30

As our products undergoes continuous development the specifications are subject to change without prior notice

INDEX

1. Product Information

1.1 Product brief

Thank you for purchasing DIGISOL DG-LB1054 enterprise routers (in the following text, referred to as the product). DG-LB1054 can access a variety of ISP line, meeting your different needs. It supports multiple WAN traffic load balancing and line redundancy backup, broadband connections to achieve the highest efficiency.

DG-LB1054 provides a highly efficient network security using its powerful features like firewall, filtering illegal requests to the server in LAN, filtering hackers on a local area network IP address and port scanning to prevent malicious attacks from outside. Also by using IP address and MAC address binding it prevents IP address spoofing, making your network more secure and stable.

DG-LB1054 has Web Interface for all features making user experience simple.

DG-LB1054 provides WAN port, you can directly connect more than one incoming line, doubling bandwidth and can connect to a different ISP, and you can simultaneously play a backup role and load sharing.

It has WEB interface for LAN traffic monitoring and management.

1.2 Main features and specifications of the product

1.2.1 Main Features

- Supports IP address and MAC address binding preventing address theft.
- Real-time monitoring: Displays users within LAN traffic and connection lines, detects network anomalies as well as abnormal users.
- Firewall protection: Monitors Internet traffic, filtering illegal requests to the server in LAN, filter hacking software on a local area network IP address and port scanning to prevent malicious attacks from outside, preventing DOS/DDoS attacks.

- Set the administrator password which prevents unauthorized users to modify router configuration. Using backup configuration file, you can prevent the accidental loss of configuration.

2. Bandwidth management

- Supports bandwidth sharing.
- Network bandwidth control, restricts bandwidth intensive P2P traffic.

3. Configuration and management

- Graphical WEB configuration interface with easy management and configuration.
- Remote management: Any one computer on a local area network or a wide area network can be restricted for remote administration.

4. Advanced features

- DG-LB1054 supports the high performance intelligent flow control function.
- Unique VPN features, allowing private LAN user connectivity through secured tunnel.
- Supports PPPoE Server, for connecting PPPoE dial-up users and can speed limits for each account along with billing management.
- Supports WEB certification for different users, giving you more choices.

5. WAN port (WAN)

- WAN port (WAN): Integrated 10/100Mbps port (MDI/MDI-X).
- Share Internet access, support multiple ISP access, policies based on destination address mode, supports multiple WAN traffic load sharing and link redundancy backup, all LAN users to NAT (Network Address Translation) to share Internet access.
- Supports DSL or Cable Modem. Supports the use of PPPoE (PPP over Ethernet) protocols for ISP connection.
- Supports fixed & dynamic IP address for Ethernet access.

- DMZ/WAN2 port: Integrated 10/100Mbps port, separate DMZ network segment and WAN port cooperation supporting traffic load sharing and link backup.

6. LAN ports (LAN)

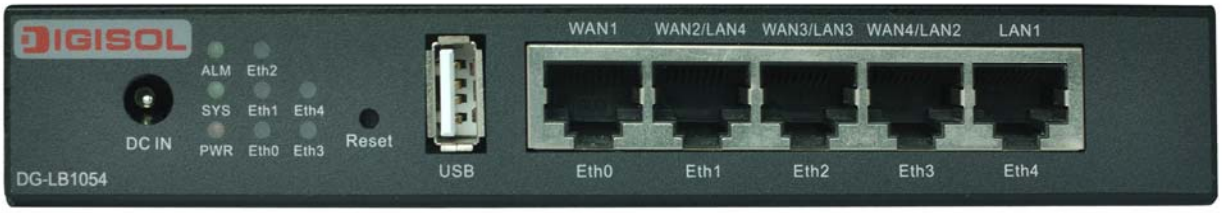
- Integrated multi-port 10/100Mbps switch.
- Dynamic Host Configuration Protocol (DHCP) service dynamically allocates IP address and the gateway, DNS Server and so on to computers in a local area network.

1.2.2 Product specifications

- IEEE802.3 Ethernet and IEEE802.3u Fast Ethernet standard.
- Supports TCP/IP, PPPoE, DHCP, ICMP, NAT, static routing.
- Supports auto-negotiation function, automatically adjusts the transmission and transfer speed.
- Operating environment: Temperature: 0 ºC -40 ºC, Height: 0-4000m,
- Relative humidity: 10%-90%, non-condensed
- Nominal voltage: 220V
- Maximum power: 30W

2. Hardware Installation

2.1Product Image



(1) Ethernet Ports support flexible configuration so any port can be configured as WAN, LAN.

(2) RST (Reset button): Hold down for 5-6 seconds to restore to the factory settings automatically.

(3) SYS Blinking LED normal regularity, it is used to indicate that the working status is normal. When SYS long bright lights or no lights at all times represent the routing system is not working properly.

(4) PWR LED Normal state: After power on Light.

2.2 Installation notes

(1) Please do not put the router in the unstable box or table and confirm a Cabinet or table model can be enough to support the weight of the router;

(2) Confirm the Cabinet and Workbench itself has a good ventilation system. Confirm the router into the air intake and vent space to facilitate the router chassis cooling.

(3) The system router can only be installed indoor. Please ensure that the room temperature is in the range off 0°c - 45°c, humidity in10%--90% range.

(4) Make sure to provide the operating voltage matches the voltage indicated by the router.

2.3 Install a router on Tabletop

In many cases, users do not have the standard 19-inch rack; you can place the router on the table. It is recommended to place the router on a table top or workbench pads.

This method is simple and easy, but you have to pay attention to the following matters:

(1) To ensure stability and good table ground.

(2) Allow 10 cm spaces for heat dissipation around the routers.

(3) Do not place heavy objects on the router.

2.4 Connect the power adaptor

AC power cord connection:

Step 1: Make sure there is good grounding on the other end.

Step 2: Connect the Power adapter to the router power socket on the front panel and other end to the external power supply AC power outlet.

Step 3: Check the POWER LED (PWR) on the front panel of the router. Light is on which means that the power supply is connected properly.

Note: Before you power on the router, you must first connect the ground wire.

2.5 Check after the installation is complete

(1) Check the identification of the choice of power supply to the router power is consistent.

(2) Check that the Earth wire is connected.

(3) Check cables, Power supply input cable connection is correct.

2.6 Router power on start

Step1: Confirm that the external network connection and intranet connection cables are correctly connected.

Step 2: Plug in the power adapter.

Step 3: Make sure the front panel PWR led is lit.

Step 4: Please wait for around 10sec while SYS blinking LED.

Router is up and starts at this time

3. Configuration

3.1 PC Configuration

DG-LB1054 is the default IP to 192.168.0.1, subnet mask is 255.255.255.0. The settings can be changed however there will be default value as described below. PC setting steps are as follows:

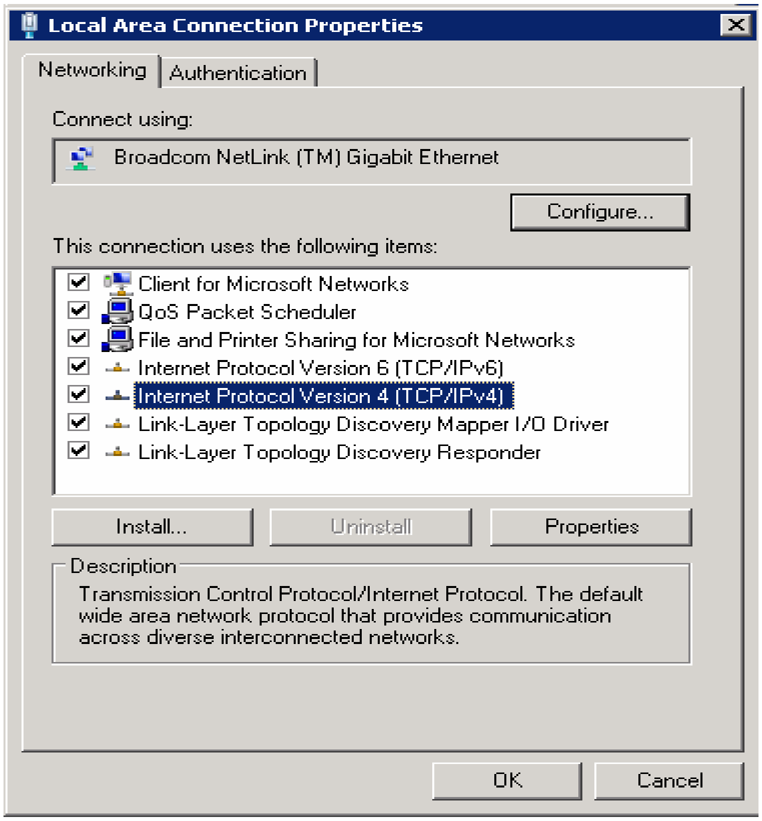
(1) The computer is connected to a port on the router.

(2) Setting up your computer IP address.

(3) Network places → view → network connections local connections.

(4) Right-click "**local area connection**" in the pop-up menu, click "**Properties**" menu.

(5) Select “**Internet Protocol (TCP/IP)** ".



Local Area Connection Properties

Networking | Authentication

Connect using:

Broadcom NetLink (TM) Gigabit Ethernet

Configure...

This connection uses the following items:

☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

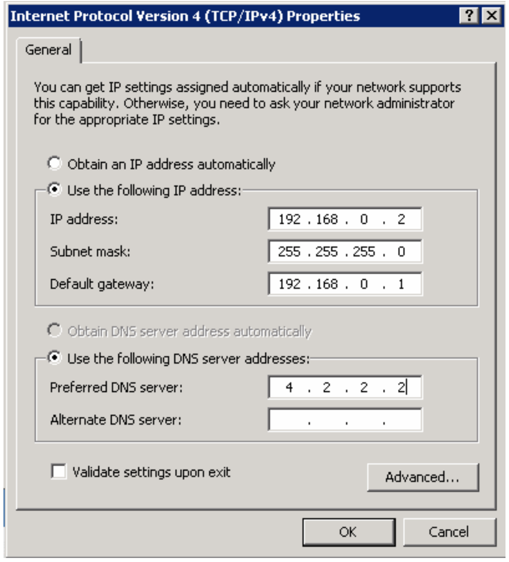
Install... | Uninstall | Properties

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK | Cancel

Click the "**Properties**" button, set the computer's IP address. Internet Protocol (TCP/IP) properties dialog box, select “**use the following IP address**", enter the “**IP address**” enter 192.168.0.xxx," subnet mask " **255.255.255.0**" default gateway fill in 192.168.0.1(The router's default IP address).



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:
IP address: 192 . 168 . 0 . 2
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 0 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: 4 . 2 . 2 . 2
Alternate DNS server: . . .

□ Validate settings upon exit

(1) Click OK to complete the configuration.

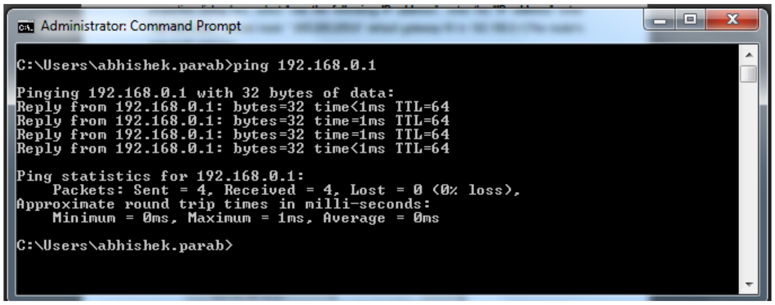
(2) Test your computer and the router is connected:

(3) Start → Run → type "**cmd** "→ enter.

(4) At the command prompt, use Ping command to test connectivity.

(5) Ping 192.168.0.1

The following display will appear if connection is successful.

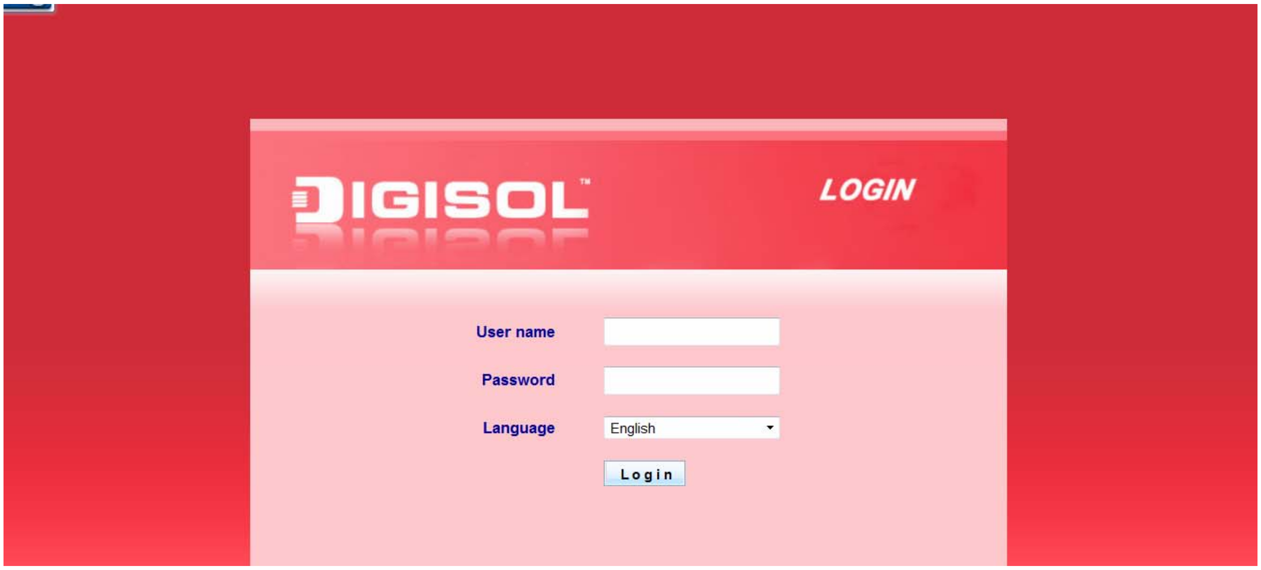


Administrator: Command Prompt

```
C:\Users\abhishek.parab>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\abhishek.parab>
```

3.2 System login

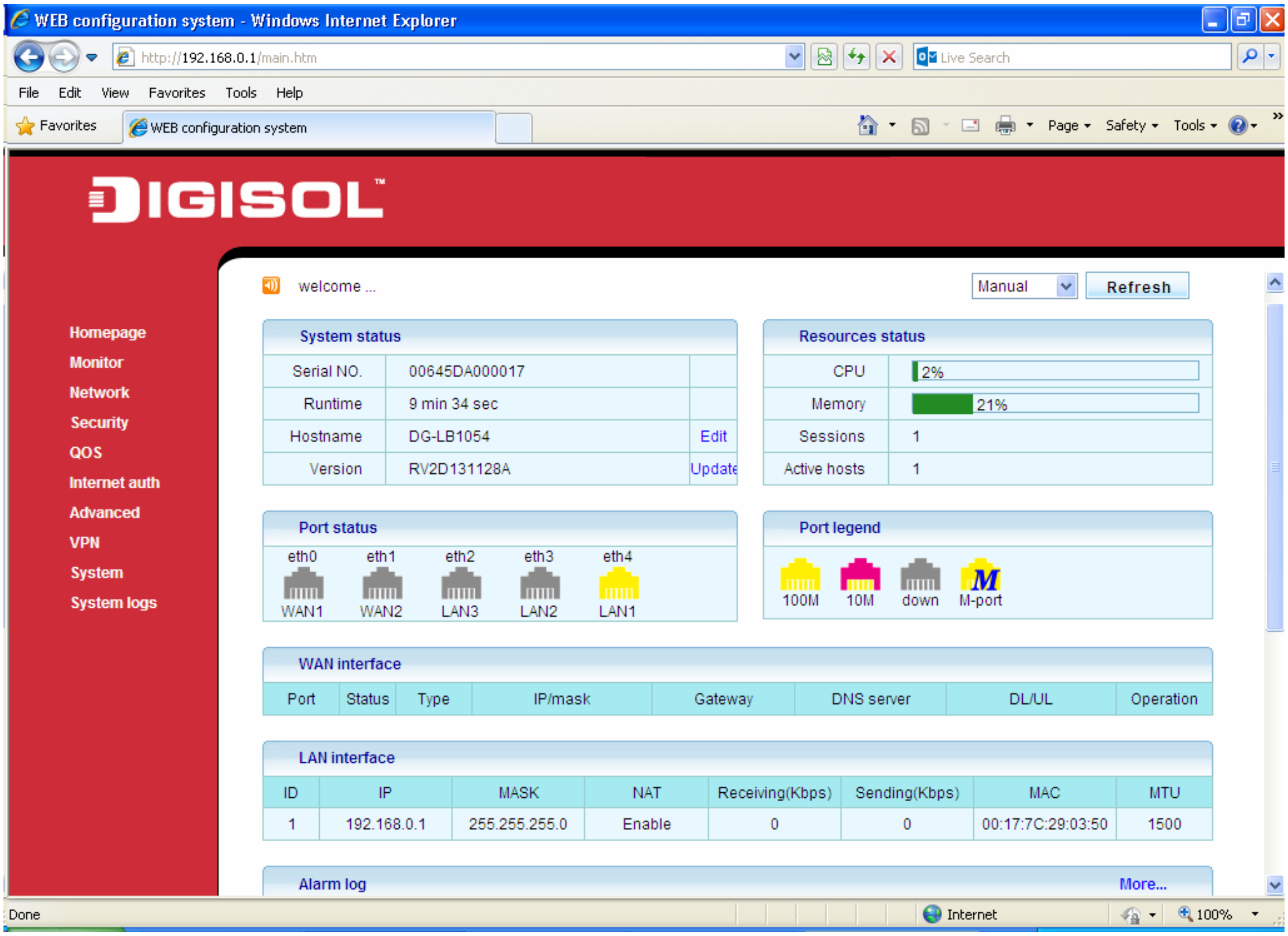
In the Internet address bar, type http://192.168.0. 1, login the router configuration interface. Login tips page is displayed as shown below:



Factory management router user name and password are “**admin**”, the default gateway is 192.168.0.1.

After you log on to the system, see the interface, as shown in the following figure. (from one model to another, there may be minor differences).

Homepage screen displays the system status of a device, including run time, host name, Serial number and firmware version. You can view the system factory information.
Resources status of the device, including CPU usage, memory usage, number of sessions and the number of active hosts, you can view in the system resource usage information.
In Port legend section, you can view the status of each port to the device. WAN and the LAN interface, allows you to understand the systems network IP address and gateway information. The alarm logs, security logs and network logs, allow you to understand system dynamics in real time.



System status

Serial NO.	00645DA000017	
Runtime	9 min 34 sec	
Hostname	DG-LB1054	Edit
Version	RV2D131128A	Update

Resources status

CPU	2%
Memory	21%
Sessions	1
Active hosts	1

Port status

eth0	eth1	eth2	eth3	eth4
WAN1	WAN2	LAN3	LAN2	LAN1

Port legend

100M 10M down M-port

WAN interface

Port	Status	Type	IP/mask	Gateway	DNS server	DL/UL	Operation

LAN interface

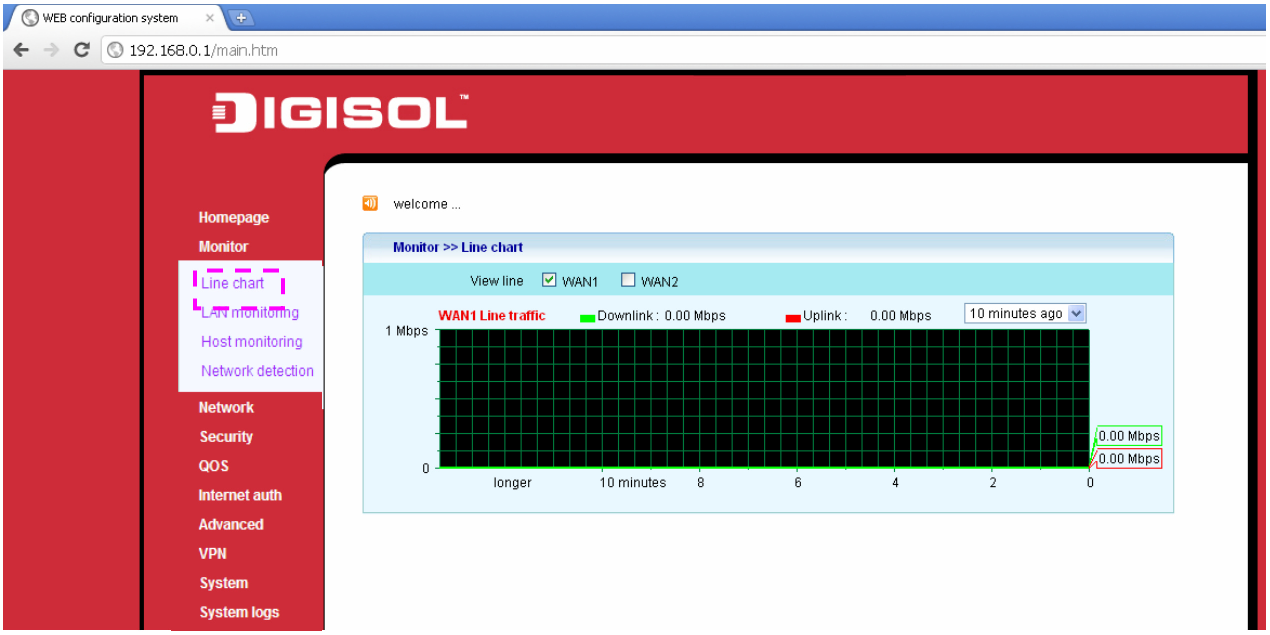
ID	IP	MASK	NAT	Receiving(Kbps)	Sending(Kbps)	MAC	MTU
1	192.168.0.1	255.255.255.0	Enable	0	0	00:17:7C:29:03:50	1500

Alarm log More...

3.3 Monitoring

3.3.1 Line chart

In the configuration page, you can see each line of the flow. Open the circuit flowchart page **WEB management interface ->Monitor ->Line chart**, as shown below:



WEB configuration system

192.168.0.1/main.htm

welcome ...

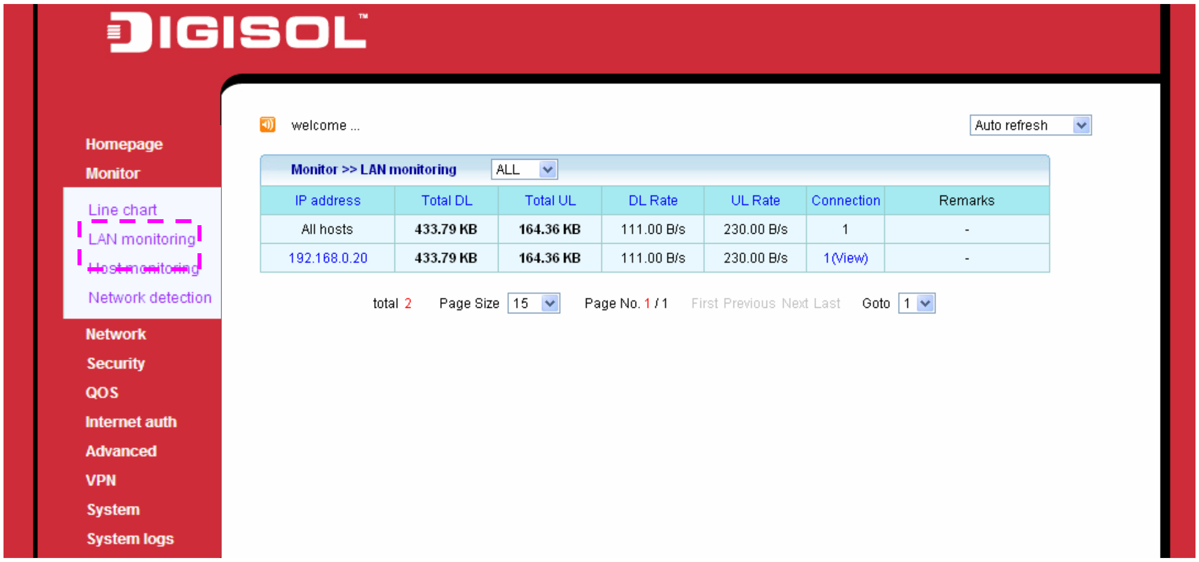
Monitor >> Line chart

View line ☑ WAN1 □ WAN2

WAN1 Line traffic 🟩Downlink : 0.00 Mbps 🟥Uplink : 0.00 Mbps 10 minutes ago

3.3.2 LAN Monitoring

In the configuration page, you can see the need to review the network host information. Open the parameters page **WEB management interface -> Monitor -> LAN Monitoring**:



Monitor >> LAN monitoring ALL

IP address	Total DL	Total UL	DL Rate	UL Rate	Connection	Remarks
All hosts	433.79 KB	164.36 KB	111.00 B/s	230.00 B/s	1	-
192.168.0.20	433.79 KB	164.36 KB	111.00 B/s	230.00 B/s	1 (View)	-

total 2 Page Size 15 Page No. 1 / 1 First Previous Next Last Goto 1

(1) Refresh: Select to automatically refresh the current flow page, or stopping the automatic page refreshes the current flow.

(2) IP address: Current intranet all host IP address.

(3) Total downloads: Current cumulative flow of every host in the intranet router to download the data.

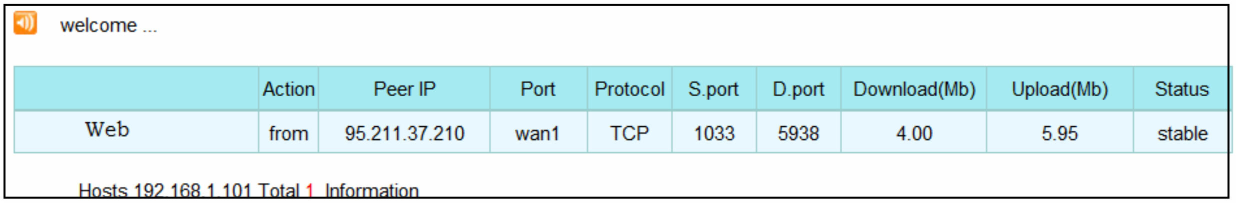
(4) Total uploaded: Current cumulative flow of each intranet host to upload data through a router.

(5) Download rate: The current speed of every host in the intranet router to download the data.

(6) Upload rate: The current intranet each host to upload data speed through a router.

(7) Connections: Current number of concurrent connections to every host in the intranet.

(8) Connection information: Click the host IP Address you can view connection information for specific hosts, as shown below:



welcome ...

	Action	Peer IP	Port	Protocol	S.port	D.port	Download(Mb)	Upload(Mb)	Status
Web	from	95.211.37.210	wan1	TCP	1033	5938	4.00	5.95	stable

Hosts 192.168.1.101 Total 1 Information

Note: (1) Click Information & wait for 2-3 seconds to refresh. Please be patient. Wait time depends on the system load. The larger the system load, longer the wait time.

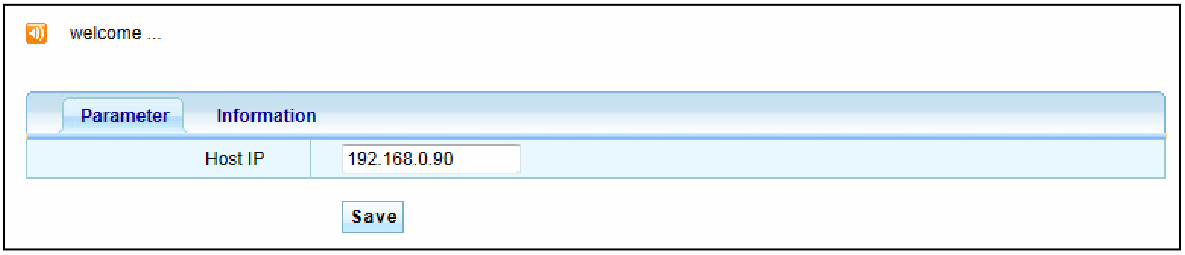
(2) Click on header to sort, remarks and IP/MAC Bound list associated notes.

3.3.3 Host monitoring

1. Parameter configuration

In the configuration page, you can define an IP address of the Host which you want to monitor. Once the host IP address is defined, all the traffic send/received from the defined host is listed in Information tab. This helps to monitor type of application user is accessing in LAN/WAN including bandwidth utilized for specific source and destination pair.

Open the parameters page **WEB management interface -> Monitor -> Host monitoring** as shown below:



welcome ...

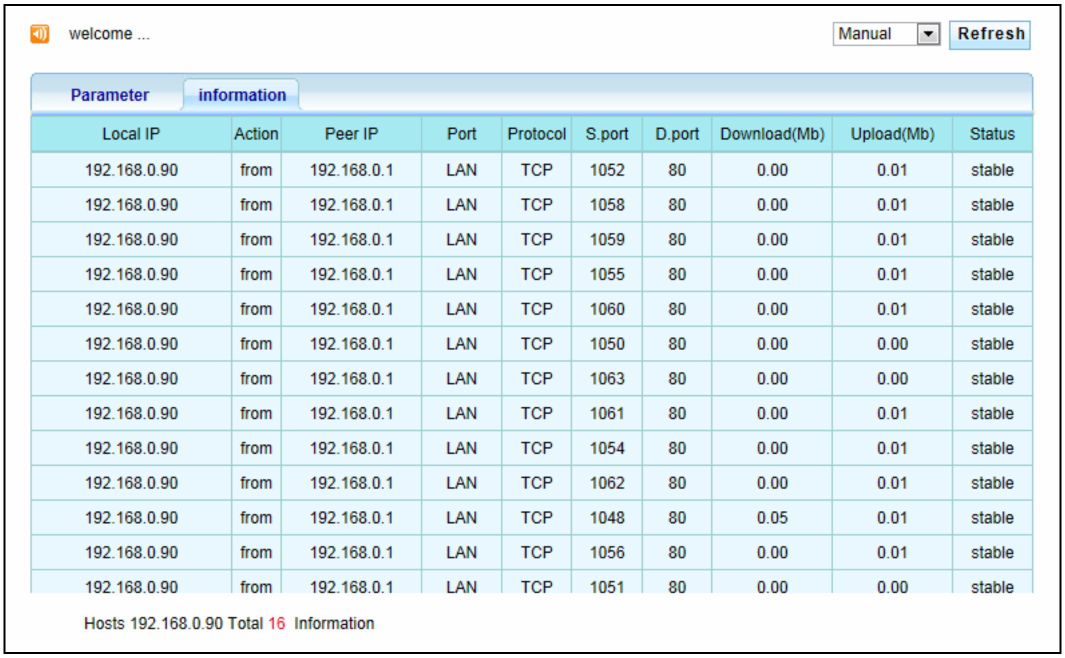
Host IP: 192.168.0.90

(1) Host IP: To monitor a host IP address.

(2) Save: Write the static configuration of the router, the parameters to take effect.

2. Connection Information

With host IP address defined on the Parameter tab, all the traffic received from defined host is listed in table below includes peer IP address, protocol type, Source/Destination Port, upload/Download utilization. Open the parameters page **WEB management interface -> network monitoring -> host monitoring -> information**, as shown below:



Local IP	Action	Peer IP	Port	Protocol	S.port	D.port	Download(Mb)	Upload(Mb)	Status
192.168.0.90	from	192.168.0.1	LAN	TCP	1052	80	0.00	0.01	stable
192.168.0.90	from	192.168.0.1	LAN	TCP	1058	80	0.00	0.01	stable
192.168.0.90	from	192.168.0.1	LAN	TCP	1059	80	0.00	0.01	stable
192.168.0.90	from	192.168.0.1	LAN	TCP	1055	80	0.00	0.01	stable
192.168.0.90	from	192.168.0.1	LAN	TCP	1060	80	0.00	0.01	stable
192.168.0.90	from	192.168.0.1	LAN	TCP	1050	80	0.00	0.00	stable
192.168.0.90	from	192.168.0.1	LAN	TCP	1063	80	0.00	0.00	stable
192.168.0.90	from	192.168.0.1	LAN	TCP	1061	80	0.00	0.01	stable
192.168.0.90	from	192.168.0.1	LAN	TCP	1054	80	0.00	0.01	stable
192.168.0.90	from	192.168.0.1	LAN	TCP	1062	80	0.00	0.01	stable
192.168.0.90	from	192.168.0.1	LAN	TCP	1048	80	0.05	0.01	stable
192.168.0.90	from	192.168.0.1	LAN	TCP	1056	80	0.00	0.01	stable
192.168.0.90	from	192.168.0.1	LAN	TCP	1051	80	0.00	0.00	stable

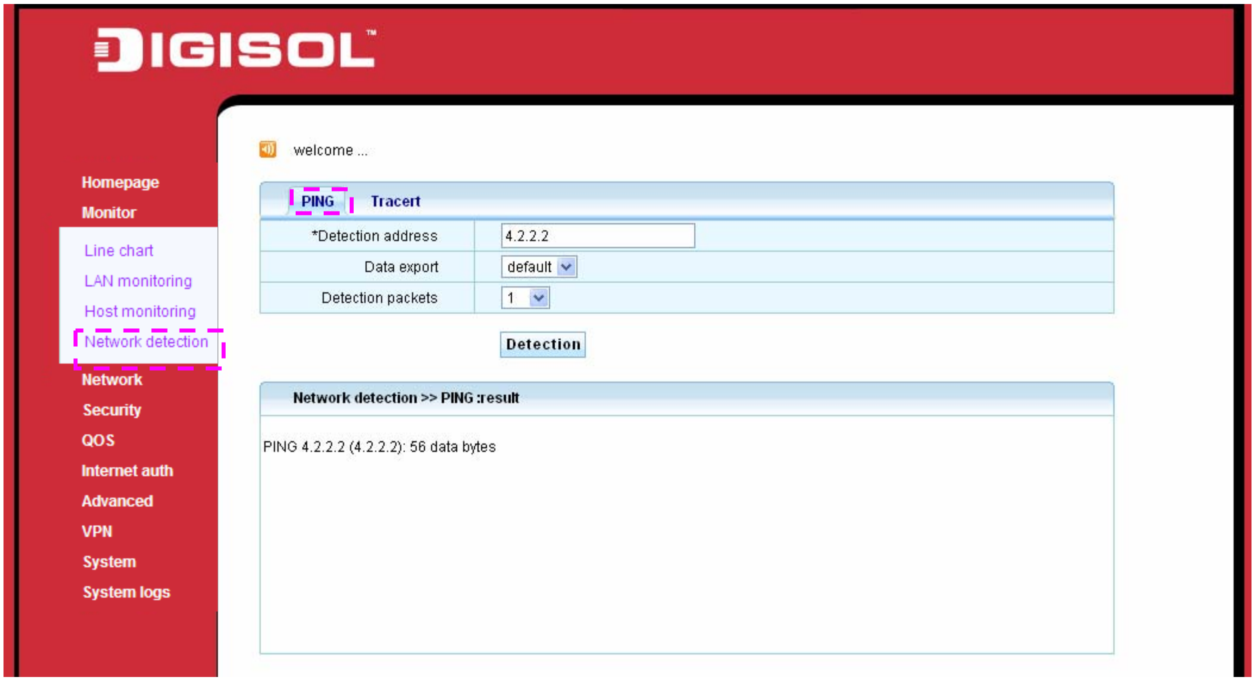
Hosts 192.168.0.90 Total 16 Information

3.3.4 Network detection

1. Ping test

In this page, you can send an ICMP Packet to a specified host through the system to monitor network performance and quality output results.

Open Ping test configuration page **WEB management interface -> Monitor-> Network Detection->Ping**, as shown below:



*Detection address: 4.2.2.2
Data export: default
Detection packets: 1

Network detection >> PING :result

```
PING 4.2.2.2 (4.2.2.2): 56 data bytes
```

(1) Detection address: The system sends ICMP packet's destination host.

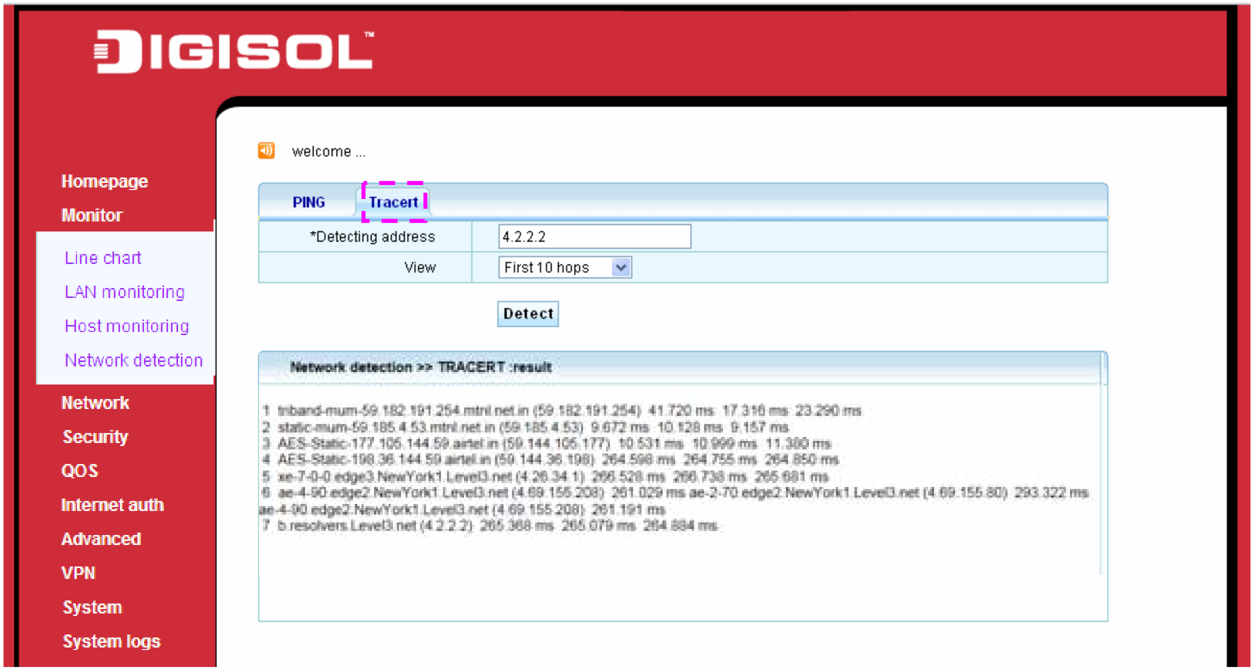
(2) Data export: Use the default, or manually select the ICMP Send export package.

(3) Detection Packets: The system sends ICMP packet number, this number is 1, 3, 5 and 10.

(4) Detection: Notify that the system starts sending ICMP packets.

2. The Tracert test

Open configuration page **WEB management interface -> Monitor -> Network detection ->Tracert**, as shown below:



*Detecting address: 4.2.2.2

View: First 10 hops

Network detection >> TRACERT :result

```
 1  triband-mum-59.182.191.254.mtnl.net.in (59.182.191.254)  41.720 ms  17.316 ms  23.290 ms
 2  static-mum-59.185.4.53.mtnl.net.in (59.185.4.53)  9.672 ms  10.128 ms  9.157 ms
 3  AES-Static-177.105.144.59.airtel.in (59.144.105.177)  10.531 ms  10.999 ms  11.380 ms
 4  AES-Static-198.36.144.59.airtel.in (59.144.36.198)  264.598 ms  264.755 ms  264.850 ms
 5  xe-7-0-0.edge3.NewYork1.Level3.net (4.26.34.1)  266.528 ms  266.738 ms  265.681 ms
 6  ae-4-90.edge2.NewYork1.Level3.net (4.69.155.208)  261.029 ms ae-2-70.edge2.NewYork1.Level3.net (4.69.155.80)  293.322 ms
ae-4-90.edge2.NewYork1.Level3.net (4.69.155.208)  261.191 ms
 7  b.resolvers.Level3.net (4.2.2.2)  265.368 ms  265.079 ms  264.884 ms
```

(1) Detecting address: The system sends Tracert target host.

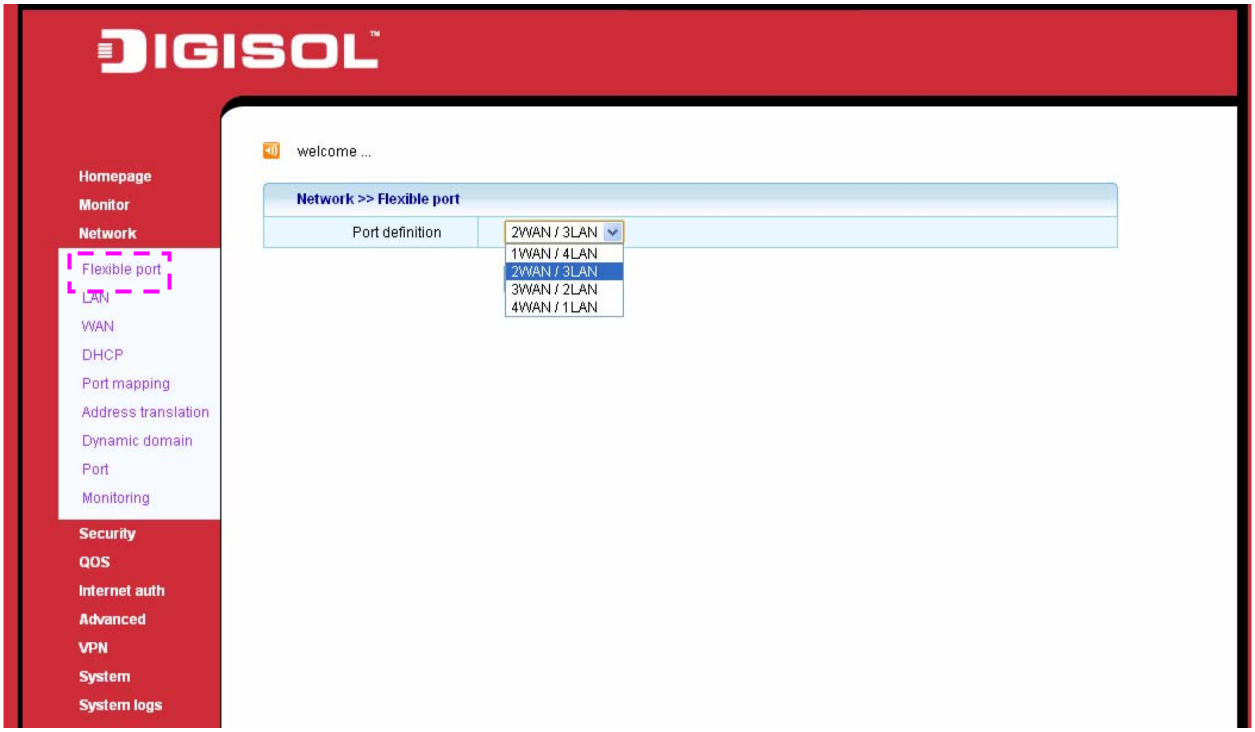
(2) View: Evaluates to 1, 3, 5 and10 jumps.

3.4 Network Configuration

3.4.1 Flexible Port

In this page, you can customize the routing WAN and LAN ports.

Open the port configuration page **WEB management interface -> Network -> Flexible port**.



Network >> Flexible port

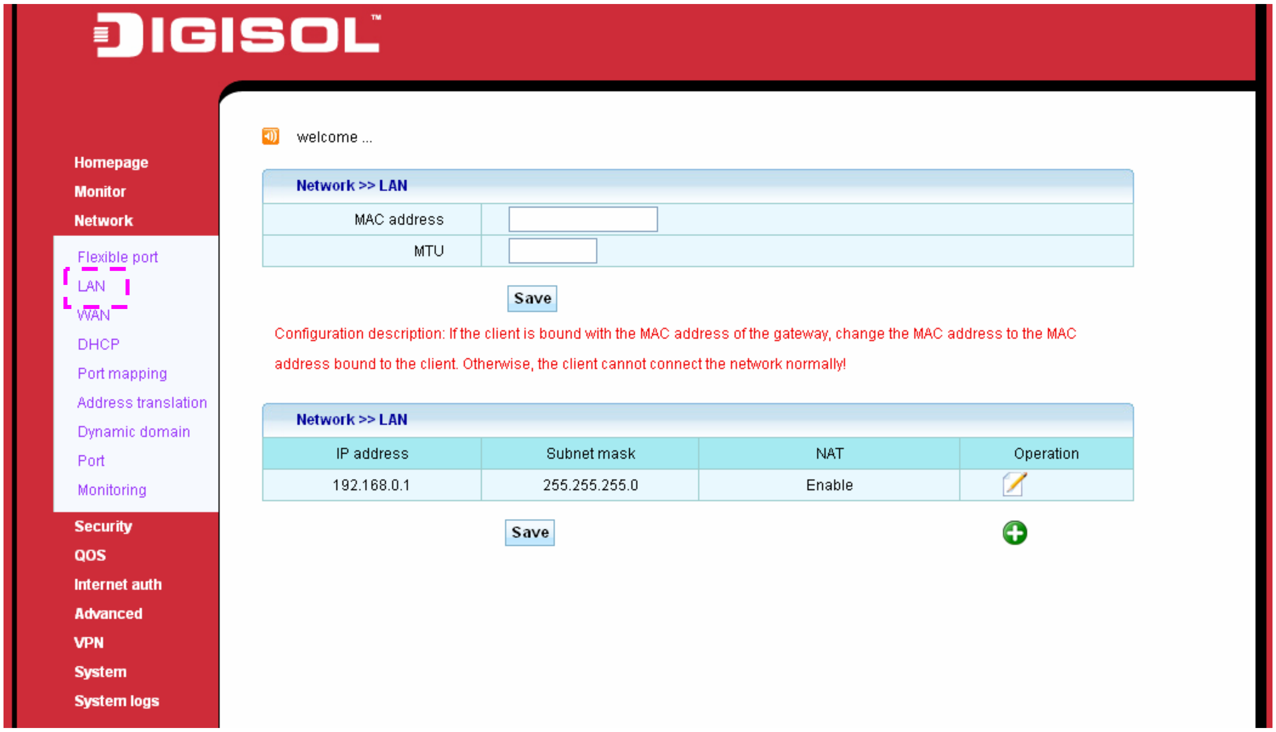
Port definition: 2WAN / 3LAN

(1) Port definition: Select WAN port and LAN port number, such as 1WAN / 4LAN represents a 1 WAN port and 4 LAN ports.

(2) Save: Write the router static configuration, then reboot the router to make the changes effective.

3.4.2 Intranet Configuration

In this page, you can modify the router LAN port TCP/IP configuration. Realization of network interconnection between the routers in LAN. Click the Network configuration link on the left **WEB management interface -> Network -> LAN.**



Network >> LAN

MAC address

MTU

Save

Configuration description: If the client is bound with the MAC address of the gateway, change the MAC address to the MAC address bound to the client. Otherwise, the client cannot connect the network normally!

Network >> LAN

IP address	Subnet mask	NAT	Operation
192.168.0.1	255.255.255.0	Enable	✎

Save

(1) MAC address: Also known as physical address, this MAC address needs to be changed when an ISP binds the customers NIC MAC address.

(2) MTU (maximum transmission unit): The default is 1500.

(3) IP address: Fill in the connection of LAN port IP address (the gateway address of your LAN). The IP address should be in the same network segment as the LAN.

(4) Subnet mask: Enter your LAN subnet mask.

(5) Network address translation: English abbreviations NAT, It allows to share single WAN IP address to different LAN/DMZ IPs.

(6) Click "**Save**", written to the static configuration of the router, the parameter to take effect and complete the configuration.

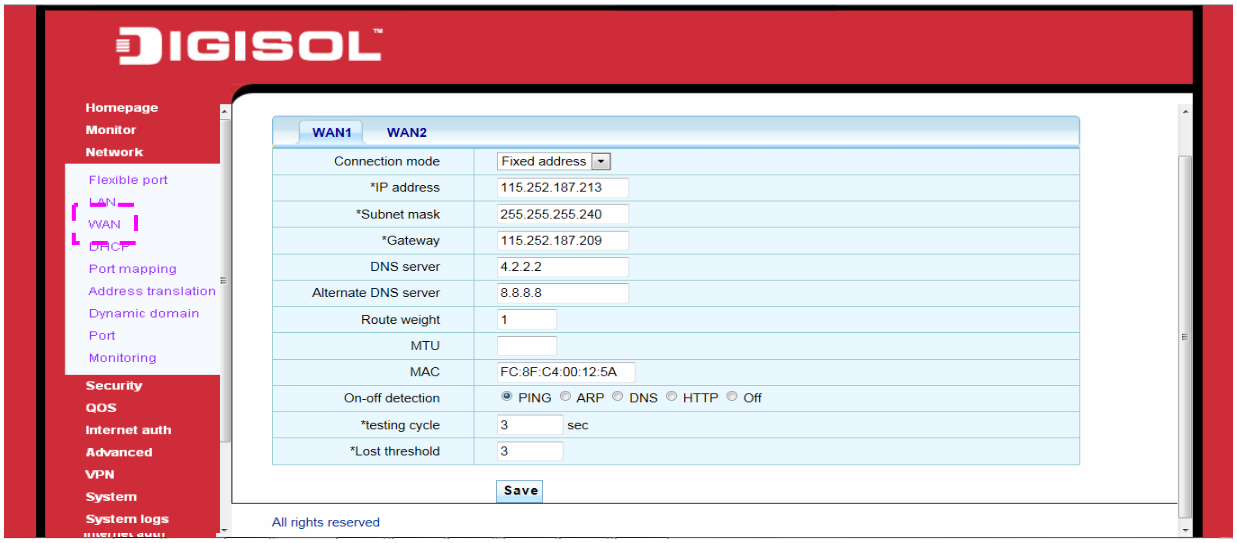
Tip: When the hosts within a subnet are all public network IP address, disable network address translation.

Note: After saving, all configurations with immediate effect, you do not have to restart.

3.4.3 WAN Network Configuration

In this page, you can use the WAN menu to select WAN port configuration. Due to identical WAN port configuration, we will explain here WAN1 configuration.

Click the left "**Network configuration → WAN Configuration**" link on the right side displays the appropriate configuration page:

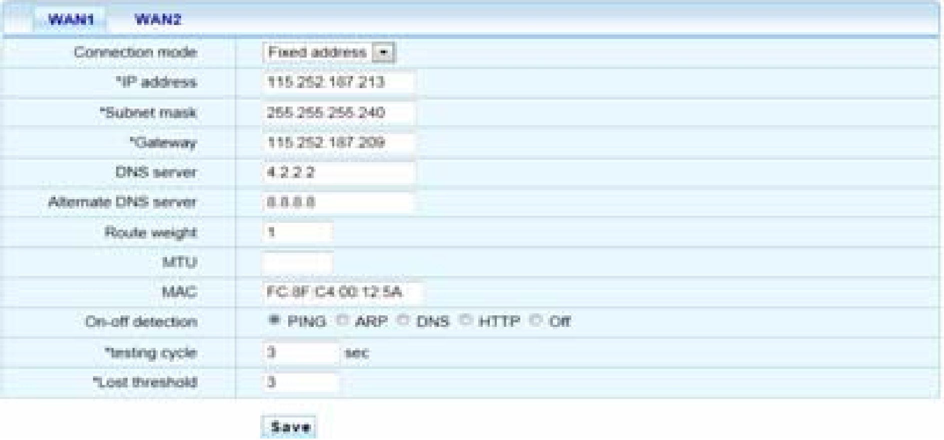


Connection mode	Fixed address
*IP address	115.252.187.213
*Subnet mask	255.255.255.240
*Gateway	115.252.187.209
DNS server	4.2.2.2
Alternate DNS server	8.8.8.8
Route weight	1
MTU	
MAC	FC:8F:C4:00:12:5A
On-off detection	● PING ○ ARP ○ DNS ○ HTTP ○ Off
*testing cycle	3 sec
*Lost threshold	3

Page displays WAN1 Out connections (such as PPPOE, fixed addresses, DHCP access and No network connections).

1. Fixed address

If you are using an ISP which provides Static IP address access, you should use this configuration.



Connection mode	Fixed address ▾
*IP address	115.252.187.213
*Subnet mask	255.255.255.240
*Gateway	115.252.187.209
DNS server	4.2.2.2
Alternate DNS server	8.8.8.8
Route weight	1
MTU	
MAC	FC:8F:C4:00:12:5A
On-off detection	● PING ○ ARP ○ DNS ○ HTTP ○ Off
*testing cycle	3 sec
*Lost threshold	3

(1) IP address: ISP provides a static IP address.

(2) Subnet mask: ISP provides the subnet mask.

(3) Gateway: ISP provides the default gateway.

(4) DNS Server: ISP provides the preferred DNS Server IP address.

(5) Alternate DNS Server: ISP provides alternate DNS Server IP addresses.

(6) Routing weight: ISP routing Hop

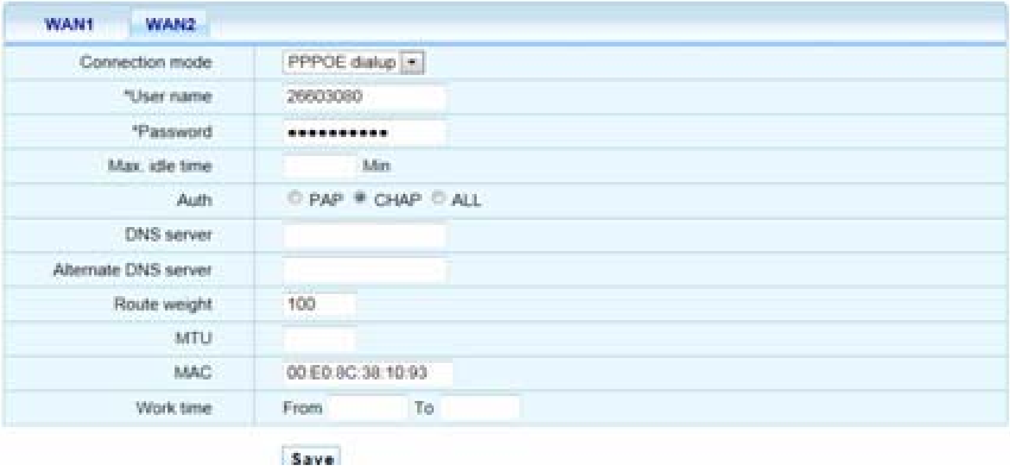
(7) MTU: (Maximum transmission unit): Defaults to 1500. Generally, not modified

(8) MAC : Also known as physical address, this MAC address is the need to replace change with Physical address of your NIC card registered with ISP.

(9) On-Off detection: When this value is present, keep alive ICMP, DNS packets are sent to Gateway to check if Link is UP.

(10) Testing Cycle: Time declare if Link is down.

2. PPPoE Dial-up (Virtual dial-up)



Connection mode	PPPOE dialup
*User name	26603080
*Password	●●●●●●●●●●●
Max. idle time	Min
Auth	○ PAP ● CHAP ○ ALL
DNS server	
Alternate DNS server	
Route weight	100
MTU	
MAC	00:E0:8C:38:10:93
Work time	From To

(1) Virtual dial-up (PPPOE): ADSL virtual dial-up (or a media over Ethernet PPPOE dial-up).

(2) User name and Password: ISP provides PPPoE Internet access account number and password.

(3) Maximum idle time: This function is intended primarily for ADSL dial-up lines that are billed on time to the user. After you enable this feature, such as intranet, Internet access requests, the system will automatically dial the connection. After reaching set value ADSL line idle time, the system will automatically hang up ADSL line, it saves Internet costs.

(4) Auth: Refers to the authentication methods. PAP authentication UNIX under the agreement or CHAP authentication Windows under the agreement. Usually selecting "**ALL**", it works.

(5) DNS server: Enter the DNS server.

(6) Alternate DNS Server: Enter the DNS server IP address provided by ISP.

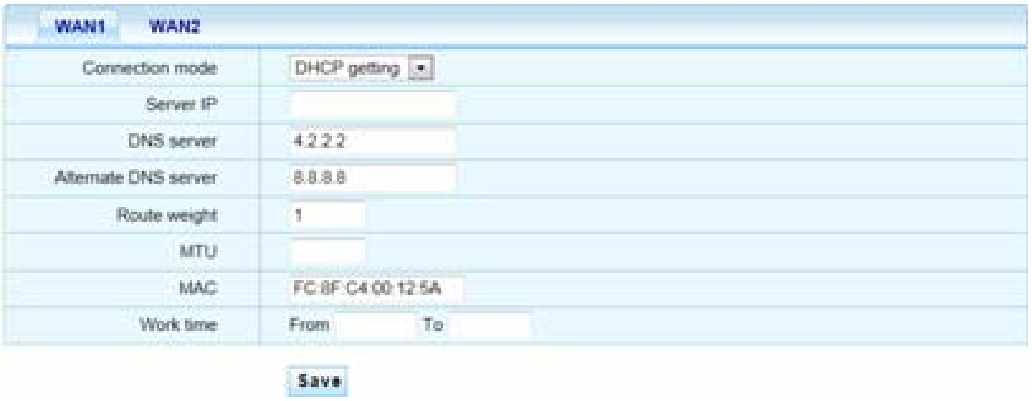
(7) MTU: Maximum transmission unit.

(8) MAC: Enter the MAC.

(9) Work Time: Enter the Time slot during which the Link will remain up.

(10) Save: Write the static configuration of the router, the parameters to take effect.

3. DHCP Getting



Connection mode	DHCP getting
Server IP	
DNS server	4.2.2.2
Alternate DNS server	8.8.8.8
Route weight	1
MTU	
MAC	FC:8F:C4:00:12:5A
Work time	From To

(1) Server IP: ISP (for example MTNL) provides IP by DHCP Server.

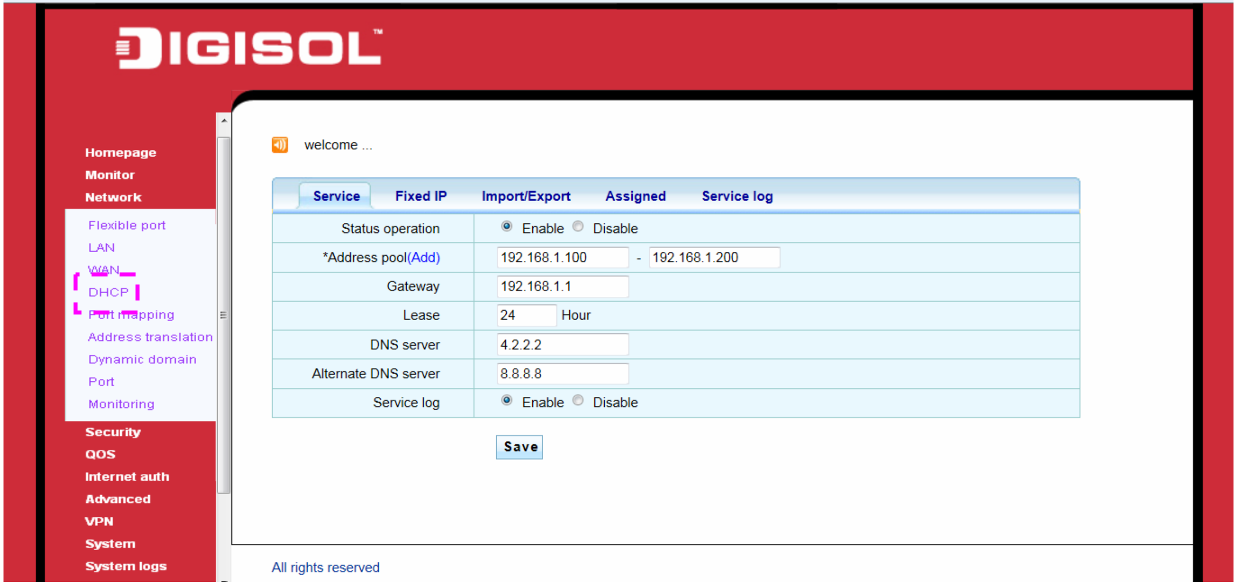
(2) Save: Write the static configuration of the router, the parameters to take effect.

4. No network connection: - Disables WAN

3.4.4 DHCP Configuration

In the configuration page, you can configure and enable system DHCP Server functionality, automatically for IP address to LAN PCs.

Open DHCP Setup page **WEB management interface -> network configuration ->DHCP**, as shown below:



Status operation ● Enable ○ Disable

*Address pool(Add) 192.168.1.100 - 192.168.1.200

Gateway 192.168.1.1

Lease 24 Hour

DNS server 4.2.2.2

Alternate DNS server 8.8.8.8

Service log ● Enable ○ Disable

(1) DHCP: Dynamic Host Configuration Protocol abbreviations, is TCP/IP protocol suite. DHCP Server is mainly used to assigned dynamic IP address, gateway Address to the network clients.

(2) Status operations: DHCP service, enable or disable.

(3) Address pool: DHCP to assign client uses all IP address ranges.

(4) Gateway: Manually specified by DHCP, provides IP address of the gateway address to the client.

(5) Lease: DHCP Server to assign client IP addresses for period.

(6) DNS Server: Assign to DHCP client computer's preferred DNS server.

(7) Alternate DNS Server: Assign to DHCP client alternate DNS server.

(8) Service log: DHCP service log ON/OFF.

(9) Save: Write the static configuration of the router, the parameters to take effect.

Note:

(1) "State actions" select "enable", the "*" identity is required.

(2) "Gateway" is left blank, the system defaults to LAN IP, and (This is usually left blank).

(3) " DNS Server" is left blank, the system defaults to LAN IP, and (This is usually left blank).

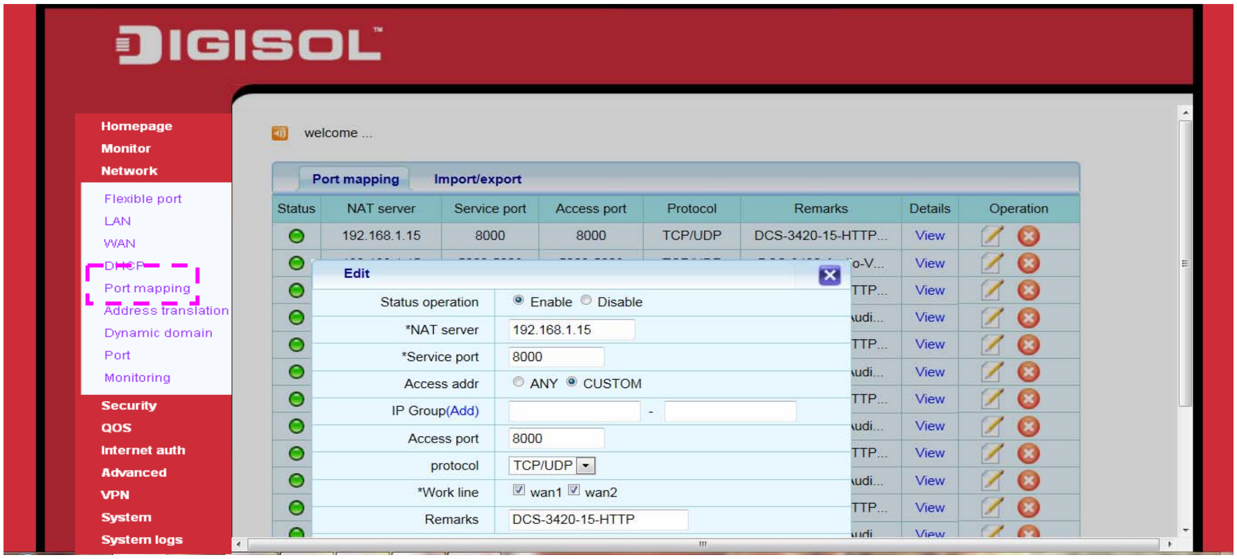
(4) "Address lease" is left blank, the system defaults to 24 hours, and (This is usually blank).

(5) DHCP Server enabled following the entry to force intranet hosts to obtain IP automatically.

3.4.5 Port Mapping

In the configuration page, you can configure a port mapping rule, so that external hosts can access your network IP specific ports to access your intranet servers so, Internet users can take full advantage of the internal network resource.

Open the port mapping configuration page **WEB management interface -> Network Configuration -> Port Mapping**, as shown below:



Status	NAT server	Service port	Access port	Protocol	Remarks	Details	Operation
●	192.168.1.15	8000	8000	TCP/UDP	DCS-3420-15-HTTP...	View	
●					o-V...	View	
●					TTP...	View	
●					udi...	View	
●					TTP...	View	
●					udi...	View	
●					TTP...	View	
●					udi...	View	
●					TTP...	View	
●					udi...	View	
●					TTP...	View	
●					udi	View	

Edit

Status operation	● Enable ○ Disable
*NAT server	192.168.1.15
*Service port	8000
Access addr	○ ANY ● CUSTOM
IP Group(Add)	-
Access port	8000
protocol	TCP/UDP
*Work line	☑ wan1 ☑ wan2
Remarks	DCS-3420-15-HTTP

(1) Port map: Also known as virtual hosting, a mechanism for achieving internal host is open to public network.

(2) The NAT (Internal server) address: To open the specified service host in the intranet IP addresses.

(3) Service port: Service port provided by the intranet server, provide different services with different service ports, ranging in value from 1-65535.

(4) Access address: You can manually specify External network IP address/range.

(5) Access port: Source port external host access to your internal servers, and your internal server port, ranging in value from 1-65535.

(6) Transfer protocols: External host which protocol to use when communicating with your internal servers.

(7) Work line: WAN ports to use.

(8) Remarks: Written comments for easy distinguish between the different mapping rules.

(9) Save: Write a static configuration, the parameters to take effect.

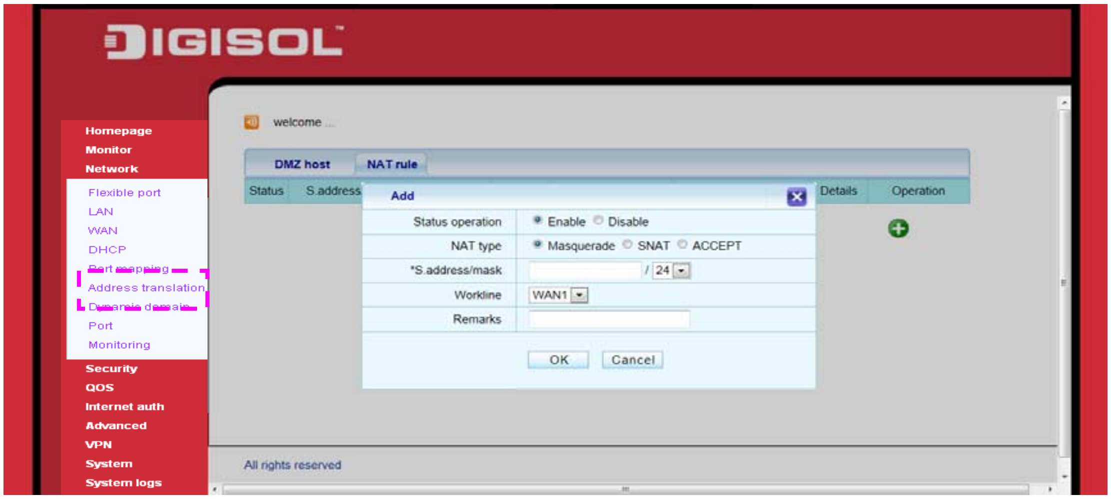
(10) Import and export: Port mapping rules can be imported or exported.

3.4.6 Address translation

1 NAT Rule

In the configuration page, you can configure address translation rules. It modifies after the router packet source IP addresses, enabling multiple users sharing one public network IP in LAN Internet access.

WEB management interface->Network Configuration->Address translation, as shown below:



Add

Status operation	● Enable ○ Disable
NAT type	● Masquerade ○ SNAT ○ ACCEPT
*S.address/mask	/ 24
Workline	WAN1
Remarks	

OK Cancel

(1) NAT type: Select a different type of address translation, when you select the Masquerade mode, fill out the address for network configuration after the conversion of the IP address, when you select the SNAT, you can manually specify a transformation after the IP address (when a wide-area network port has more than one IP Address, you can use this function) When you select ACCEPT, it selects the entire range of subnet mask.

(2) S address: Fill in your LAN IP address "/" after the mask bits, the default is 24 –bit mask.

(3) Workline: Select the Interface.

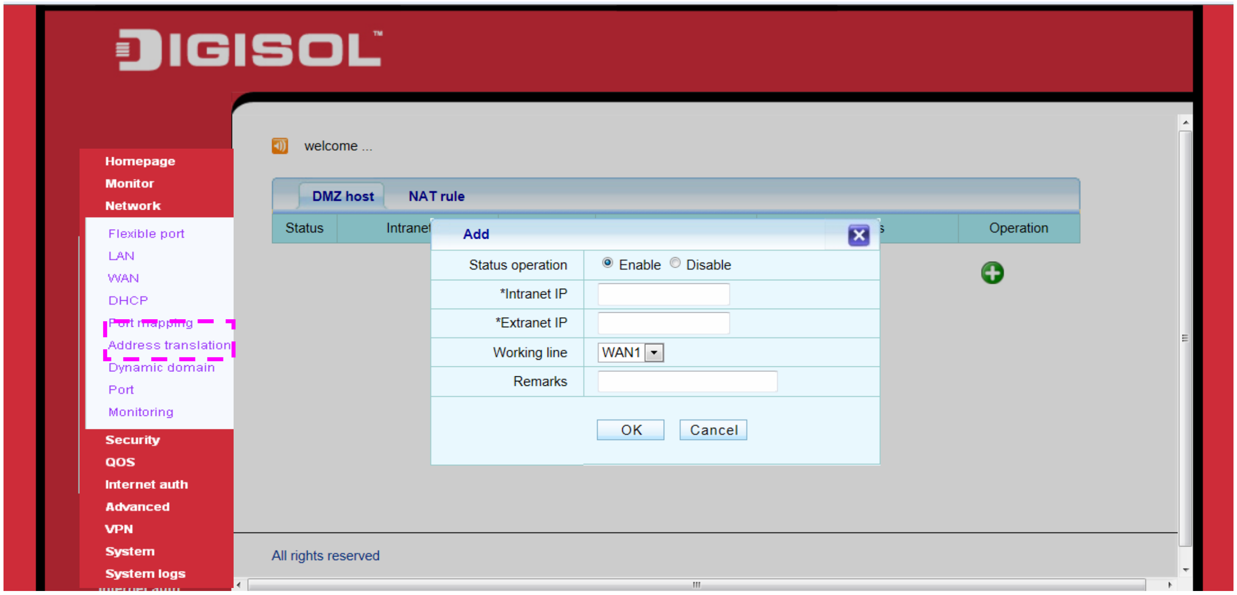
(4) Save: Write a static configuration, the parameters to take effect.

Note: With " *" Identity is required.

2 DMZ Host

In the configuration page, you can configure DMZ host rule. Internal Server can be accessed using one of External WAN IP address.

Opens the add conversion settings page **WEB management interface -> network configuration -> address translations**, as shown below:



Status operation	● Enable ○ Disable
*Intranet IP	
*Extranet IP	
Working line	WAN1
Remarks	

(1) Intranet IP: Fill in your server LAN IP address.

(2) Extranet IP: Fill in your server to use the public network IP addresses.

(3) Working line: Select the server you want to use WAN Port.

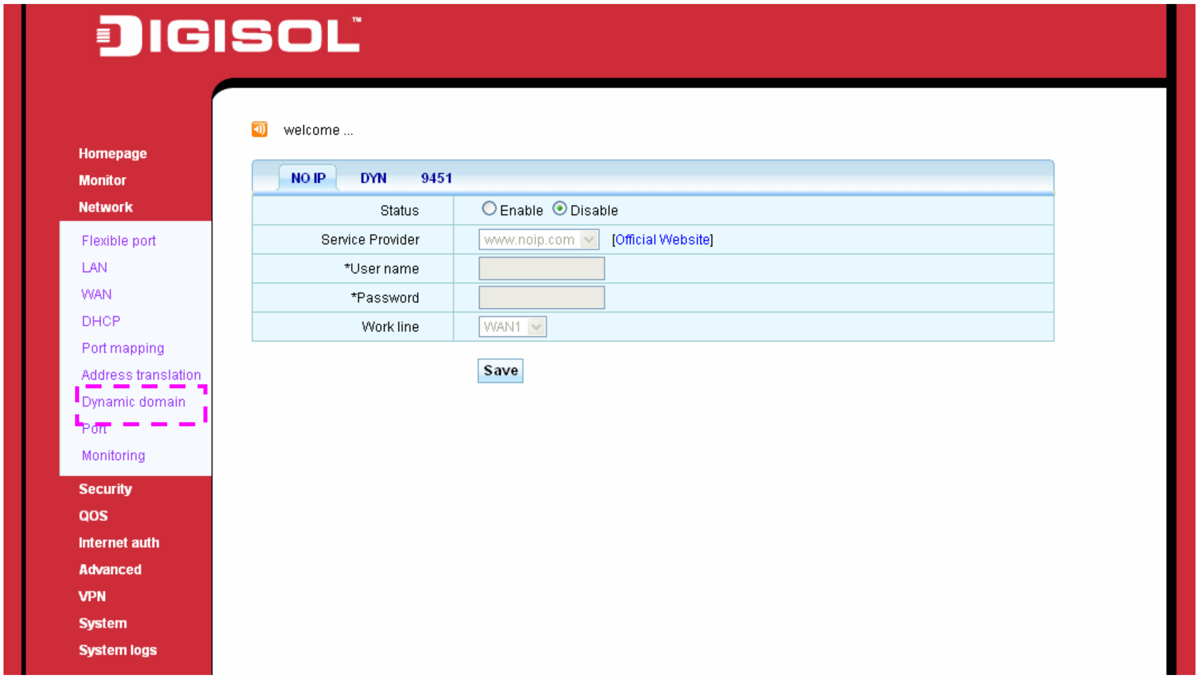
(4) Save: Write a static configuration, the parameters to take effect.

3.4.7 Dynamic Domain Name

1. NO IP

In the configuration page, you can configure dynamic DNS client parameters, dynamic DNS feature is enabled.

Open dynamic DNS settings page **WEB management interface -> Network configuration -> Dynamic Domain->NO IP**



Status ○ Enable ● Disable

Service Provider www.noip.com [Official Website]

*User name

*Password

Work line WAN1

Dynamic DNS feature: Provides a fixed domain name to a dynamic IP address resolution. Users/Router's IP address is sent to the dynamic DNS server to update the DNS database. On external Internet users browser request on this domain name, when dynamic DNS server returns the correct IP address for him.

(1) Status operation: Domain name enable/disable.

(2) Domain: Provides dynamic domain name service provider used by the domain. Such as: 9451. org

(3) Host name: Register dynamic domain name as the host name.

(4) User name: User to register dynamic domain user name;

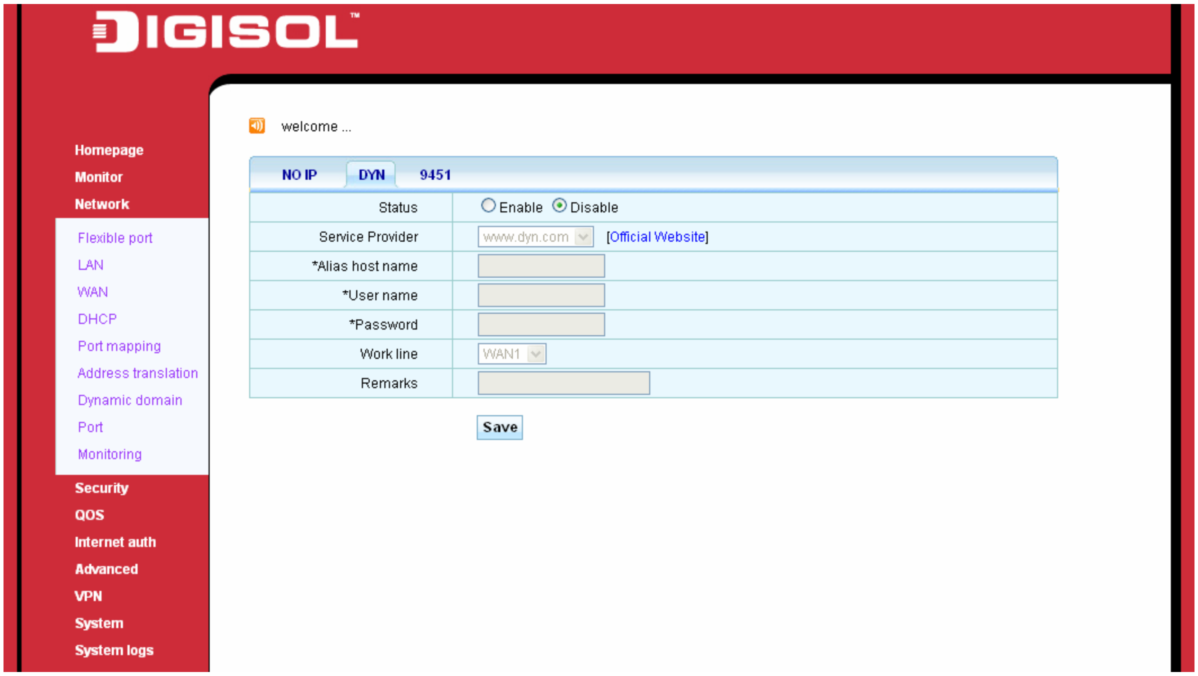
(5) Password: Password to register for dynamic domain name.

(6) Work line: WAN port selection

(7) Save: Write the static configuration of the router to take effect.

2. DYN

This page is used to configure the dynamic DNS address from Dyn.com. You can enable/disable dynamic DNS.



Status	○ Enable ● Disable
Service Provider	www.dyn.com [Official Website]
*Alias host name	
*User name	
*Password	
Work line	WAN1
Remarks	

(1) Status: Domain name enable/disable.

(2) Service Provider: Select dynamic domain name service provider from drop-down list.

(3) Host name: Registered dynamic domain name as the host name.

(4) User name: User to register dynamic domain user name

(5) Password: Password to register for dynamic domain name.

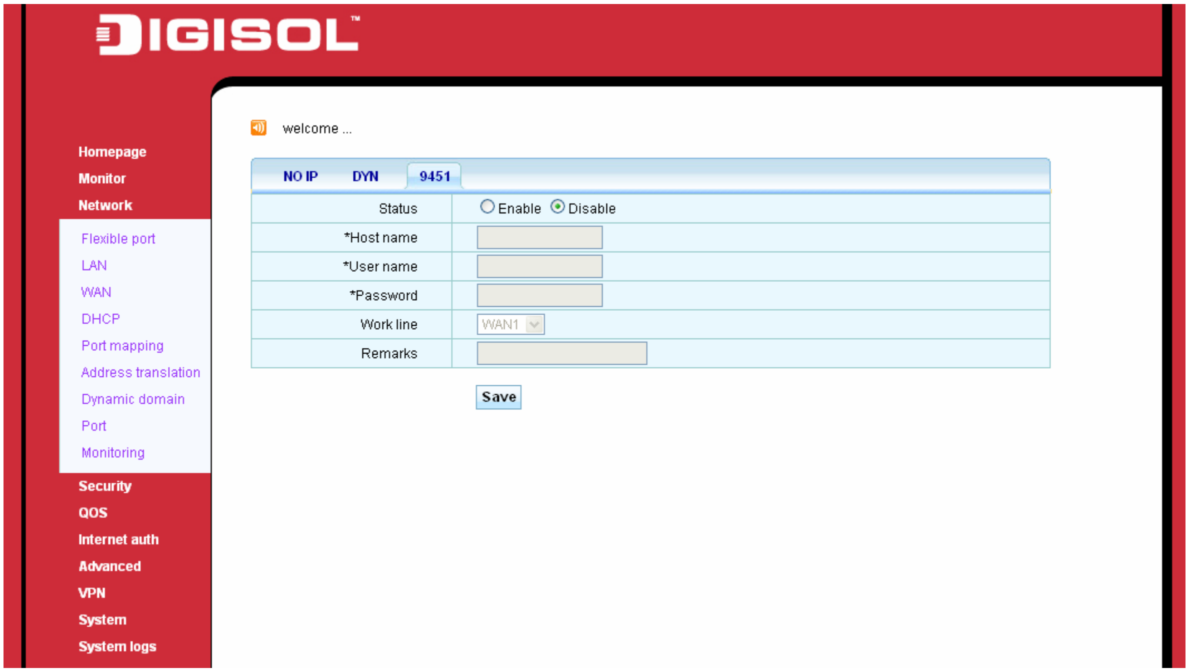
(6) Work line: WAN port selection.

(7) Remark: Add Description if any.

(8) Save: Write the static configuration of the router to take effect.

3. 9451

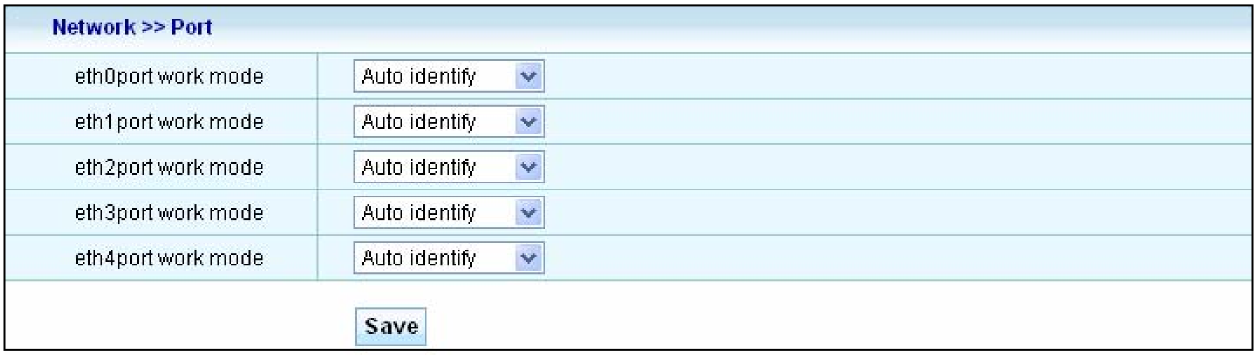
This page is used to configure the dynamic DNS address from 9451 provider. You can enable/disable dynamic DNS.



Status	○ Enable ● Disable
*Host name	
*User name	
*Password	
Work line	WAN1
Remarks	

3.4.8 Port

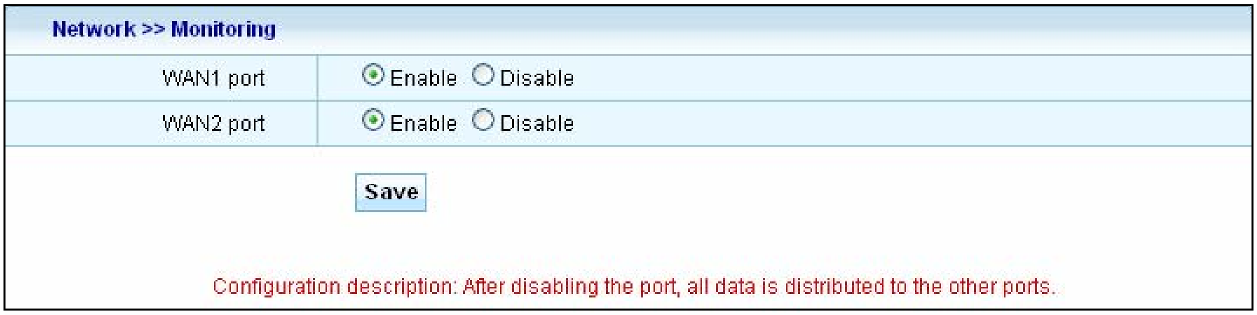
DG-LB1054 has 5 number of 10/100 mbps ports. All the ports are in Auto identify (auto-negotiations) state by default for speed-duplex parameter. Based on the type of device connected on port, speed setting can be either set to auto detect or can be forced to 10/100Mbps Half/Full Duplex.



Network >> Port

eth0port work mode	Auto identify
eth1port work mode	Auto identify
eth2port work mode	Auto identify
eth3port work mode	Auto identify
eth4port work mode	Auto identify

3.4.9 Monitoring



Network >> Monitoring

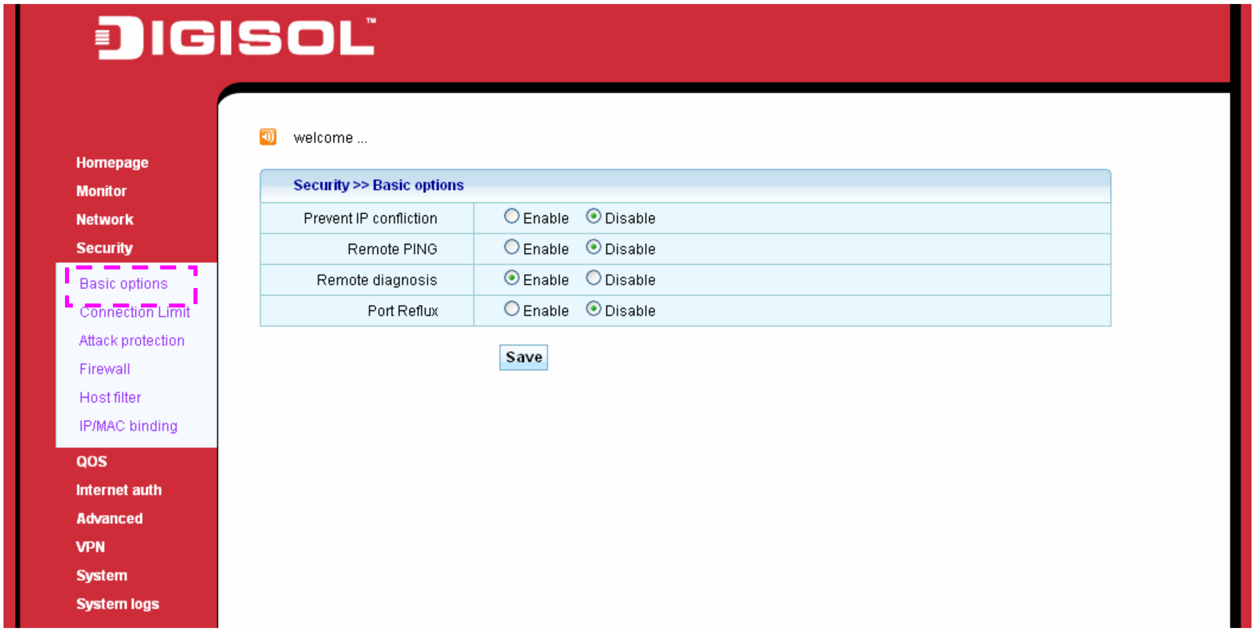
WAN1 port	● Enable ○ Disable
WAN2 port	● Enable ○ Disable

Configuration description: After disabling the port, all data is distributed to the other ports.

3.5 Security

3.5.1 Basic Options

Open the dynamic DNS settings page **WEB management interface->Security->Basic options**, as shown below:



Security >> Basic options	
Prevent IP confliction	○ Enable ● Disable
Remote PING	○ Enable ● Disable
Remote diagnosis	● Enable ○ Disable
Port Reflux	○ Enable ● Disable

(1) Prevent IP confliction: LAN hosts may be incorrectly set to and the same as the network address of the router IP address which causes a conflict that affects the network. Enable the "prevent IP conflicts" feature; you can protect the intranet address of the router.

(2) Remote PNG: You can set the router's WAN port response to the network PING requests from outside host.

(3) Remote diagnostics: Turn on or off.

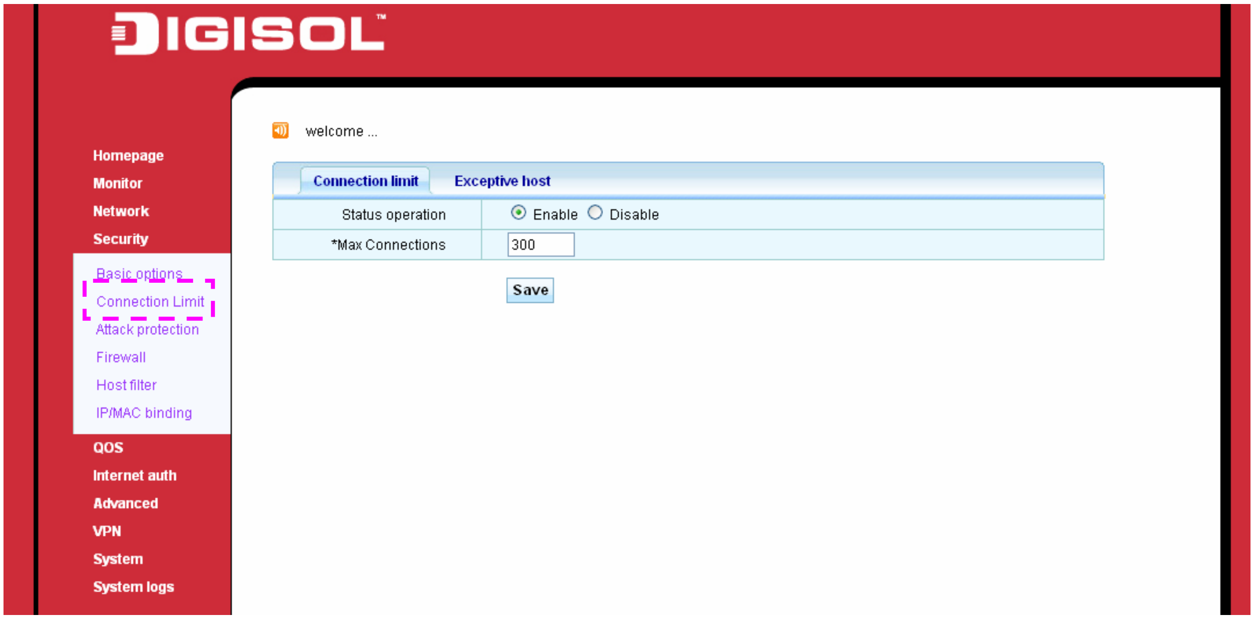
(4) Port reflux: Turn on or off. LAN host will be able to manage internal resource through WAN IP.

(5) Save: Write to the static configuration of the router to take effect.

3.5.2 Connection Limit

In this page you can configure the connection limit to specify the maximum number of concurrent connections to a single machine. When you reached the maximum number of connections, the router will refuse new connections for this client request.

Open the connection restriction profiles page **WEB management interface->Security-> connection limit**, as shown below:

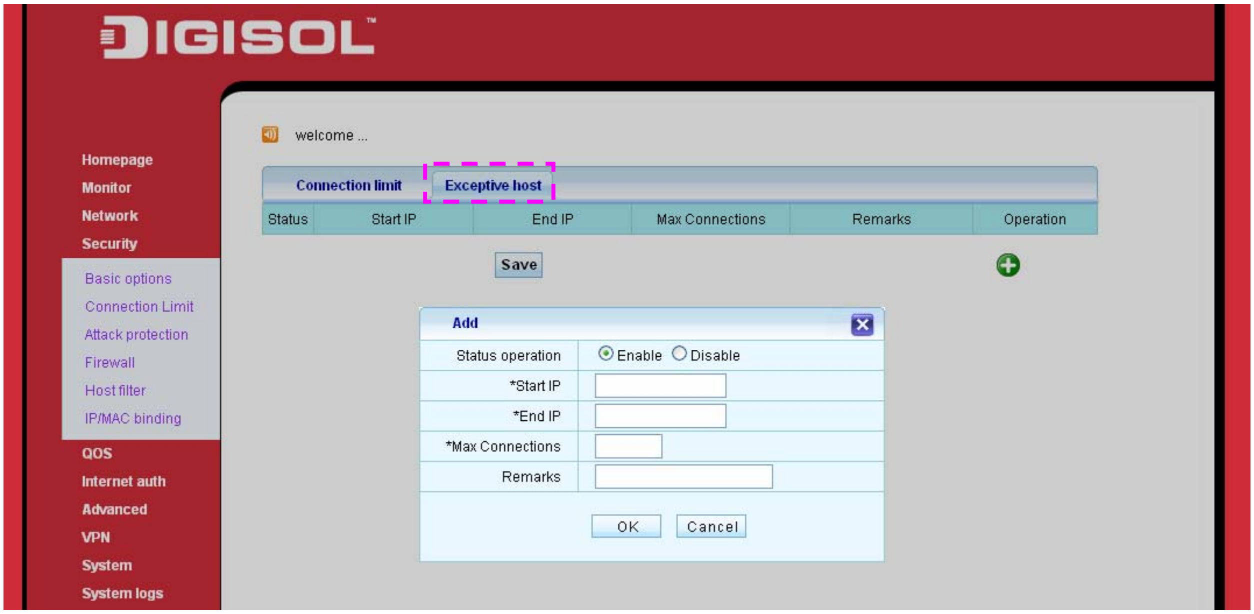


Status operation	● Enable ○ Disable
*Max Connections	300

(1) Status operation: Set the connection limit feature. It is enabled or disabled.

(2) Maximum number of concurrent connections: Set the largest TCP/IP sessions from each client at the same time.

Exceptive host: This option can be set individually for a specific client connection limit settings in the following figure:



Status	Start IP	End IP	Max Connections	Remarks	Operation

Status operation	● Enable ○ Disable
*Start IP	
*End IP	
*Max Connections	
Remarks	

(1) Status operation: Enable or disable a rule set.

(2) Start IP: Sets the exception host’s starting IP value.

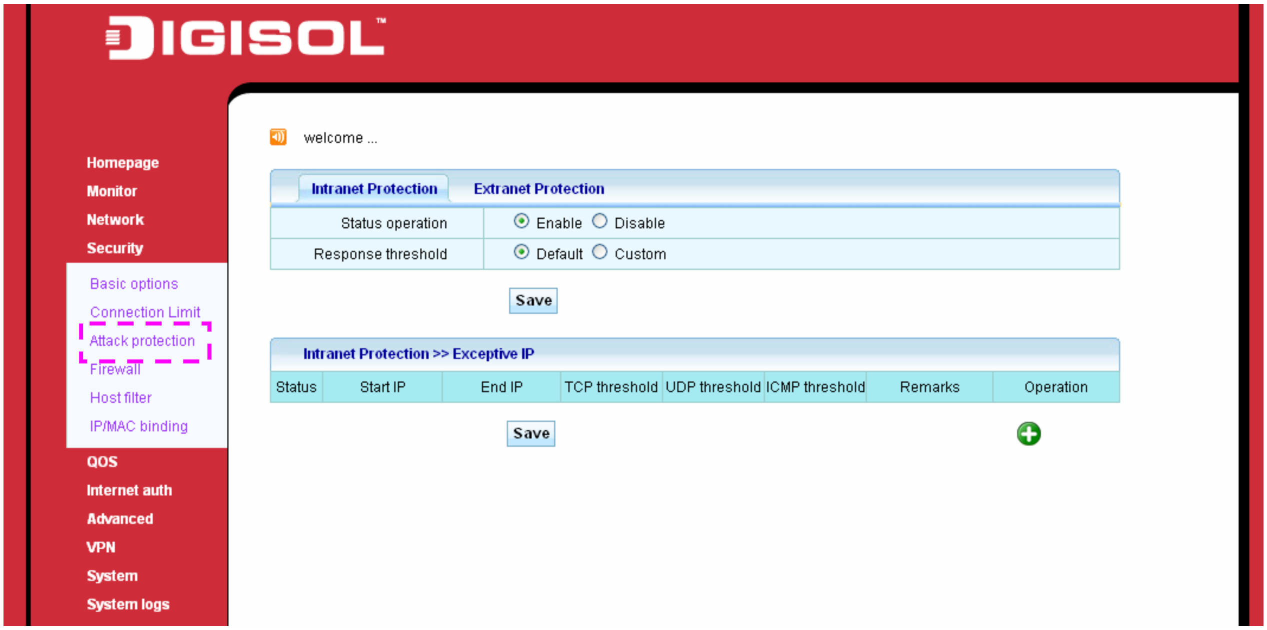
(3) End IP: Set the exceptional hosts End IP.

(4) The maximum number of connections: Set specific clients largest TCP/IP sessions.

3.5.3 Attack Protection

1 Intranet defense

In this page, you can modify "**Intranet/LAN Protection**" service status for DDoS attack detection and prevention.
Open intranet defense configuration page **WEB management interface ->Security ->Attack protection**, as shown below:



Status operation	● Enable ○ Disable
Response threshold	● Default ○ Custom

Intranet Protection >> Exceptive IP

Status	Start IP	End IP	TCP threshold	UDP threshold	ICMP threshold	Remarks	Operation

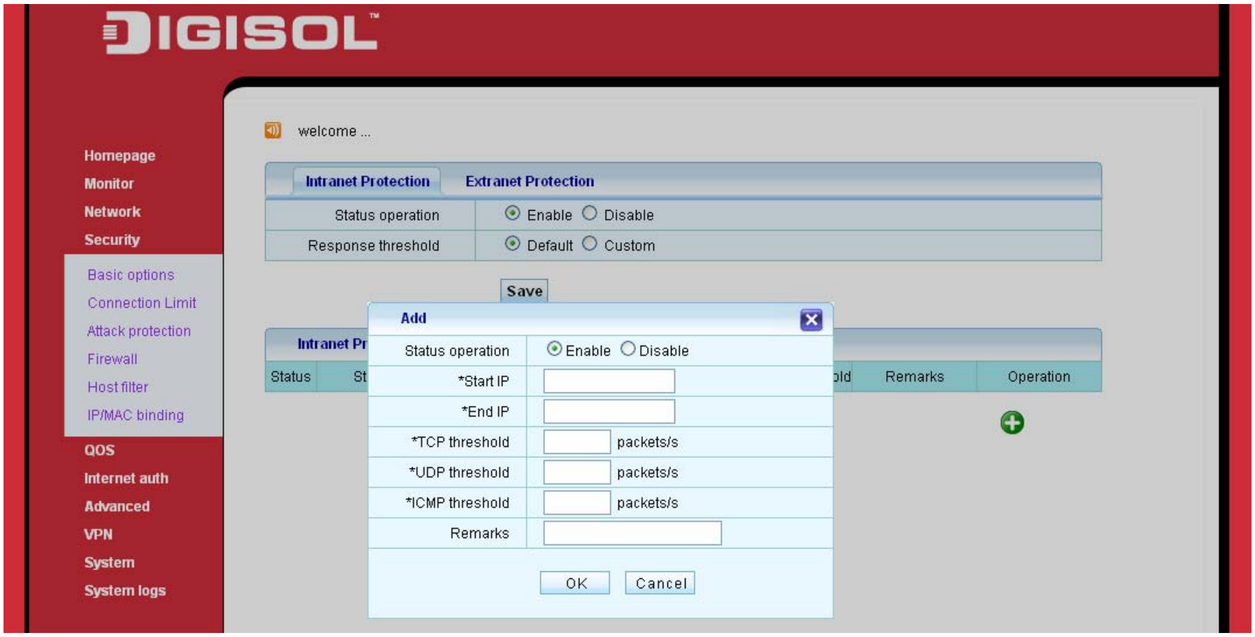
(1) Status operation: Enable or disable the protection. Response Threshold setting.

(2) TCP threshold: Allows TCP packets per second (Number ranging in value from 100-9000).

(3) UDP threshold: Allows UDP packets per second (Number ranging in value from 100-9000).

(4) ICMP threshold: Allows ICMP packets per second (Number ranging in value from 100-9000).

Click on the “**+**” sign the screen shown below will appear.



Status operation	● Enable ○ Disable
Response threshold	● Default ○ Custom

Add

Status operation	● Enable ○ Disable
*Start IP	
*End IP	
*TCP threshold	packets/s
*UDP threshold	packets/s
*ICMP threshold	packets/s
Remarks	

(6) Status operations: Enable or disable the rule.

(7) Start IP and End IP: Specific IP clients Starting and Ending IP.

(8) Save: Write the static configuration of the router, the parameters to take effect.

Note:

(1) TCP-FLOOD package when the threshold value is present, must be a number from 100-9000.

(2) UDP-FLOOD thresholds exist, must be a number from 100-9000.

(3) ICMP-FLOOD thresholds exist, must be a number from 100-9000.

(4) Other package rate value must be greater than 0 integers.

2 Extranet (WAN side) defense

(1) WAN1 Response connection threshold: Maximum value routers WAN1 can handle for network connections per second.

(2) WAN2 Response connection threshold: Maximum value routers WAN2 can handle for network connections per second.

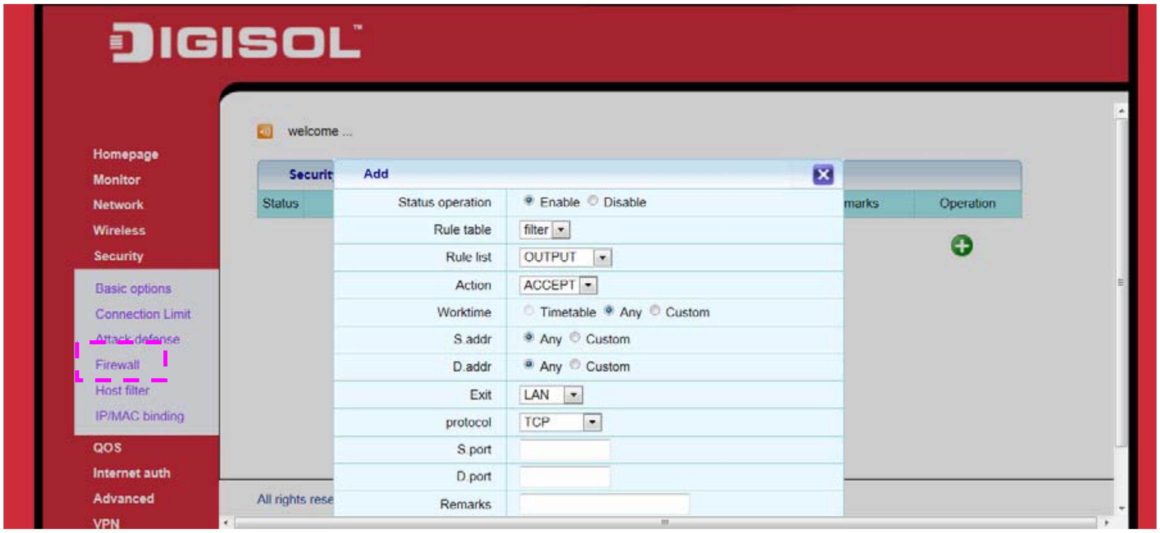
(3) Save: Write the static configuration to the router.

Note: The Response rate values that exist, must be a number from 512-999999, (Recommended values 1000).

3.5.4 Firewall

In this page, you can configure the firewall feature to allow or disallow matching packets to pass through.

Open the firewall settings page **WEB management interface ->Security ->Firewall**, as shown below:



Add

Status operation	● Enable ○ Disable
Rule table	filter
Rule list	OUTPUT
Action	ACCEPT
Worktime	○ Timetable ● Any ○ Custom
S.addr	● Any ○ Custom
D.addr	● Any ○ Custom
Exit	LAN
protocol	TCP
S.port	
D.port	
Remarks	

(1) Status operation: Select enable or disable the current firewall rule set.

(2) Rule table: Select firewall rules table rule form, Filter and NAT in two forms, filter on behalf of

filtering, NAT on behalf of Network address transformation.

(3) Rule List: Select the firewall rules OUTPUT, INPUT, FORWARD.

(4) Action: Matching results to a specified packet, optional ACCEPT (allow) or DROP (forbidden).

(5) Working hours: The time period set up firewall rules in force.

(6) S addr: Source IP address

(7) D addr: Destination IP address

(8) Interface: Import in the packet message field, optional LAN and the WAN1, and WAN2 or arbitrary.

(9) Interface: Packet messages in the export field, optional LAN and the WAN1, and WAN2 or arbitrary.

(10) Protocol: The Protocol field in the packet is sent, the optional TCP and UDP, TCP/UDP, ICMP, GRE and ESP or arbitrary.

(11) Source port: Source port field of the packet is sent; if the field does not exist or is not required to match this field can be left blank.

(12) Destination port: Destination port field of the packet is sent, if the field does not exist or is not required to match this field can be left blank.

(13) Note: The description to a specified firewall rule.

(14) Save: Write the static configuration, the configuration to take effect.

Note:

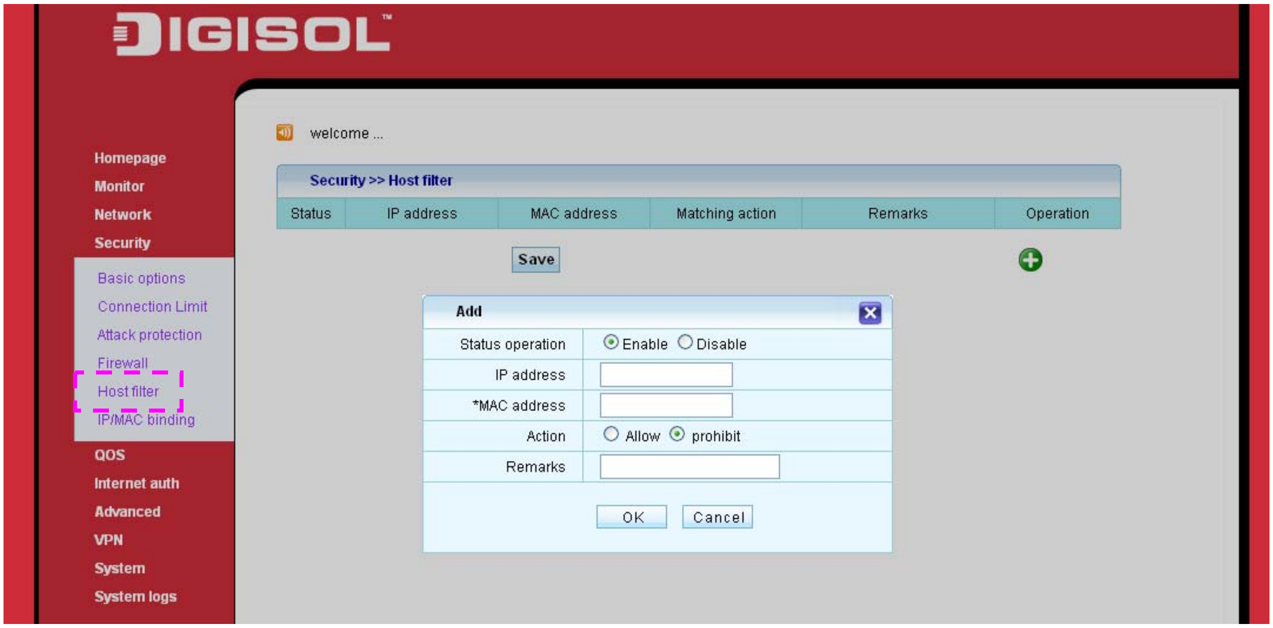
(1) For Source and destination ports only protocol options are TCP and UDP.

(2) Source port and destination port complete range 1-65535.

3.5.5 Host filters

In this page you can configure the host filtering rules, under which hosts are allowed to pass and which hosts the prohibited.

Open the host filter settings page **WEB management interface ->Security->Host filter**, as shown below:



Status	IP address	MAC address	Matching action	Remarks	Operation

Status operation	● Enable ○ Disable
IP address	
*MAC address	
Action	○ Allow ● prohibit
Remarks	

(1) Status operations: Select Enable or disable filtering rules.

(2) IP address: Host IP address.

(3) MAC address: Physical address of the network card.

(4) Action: Allow or Prohibited.

(5) Remarks: The description of the specified host filtering rules.

(6) Save: Write the static configuration, the configuration to take effect.

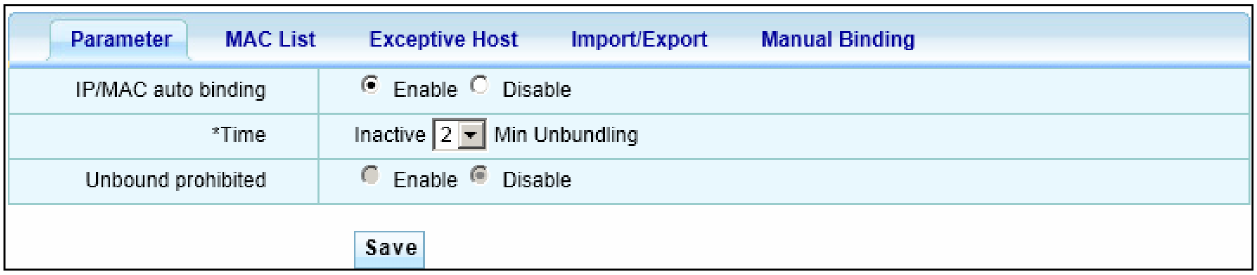
Note:

(1) "*" Identity is required.

Example: When a user is encountered with IP Address 192.168.10.2 and MAC address 00:11:22:33:44:55, then that specific user will be prohibited or allowed. If user changes its IP address then this setting will not work as it checks for exact match.

3.5.6 IP MAC Binding

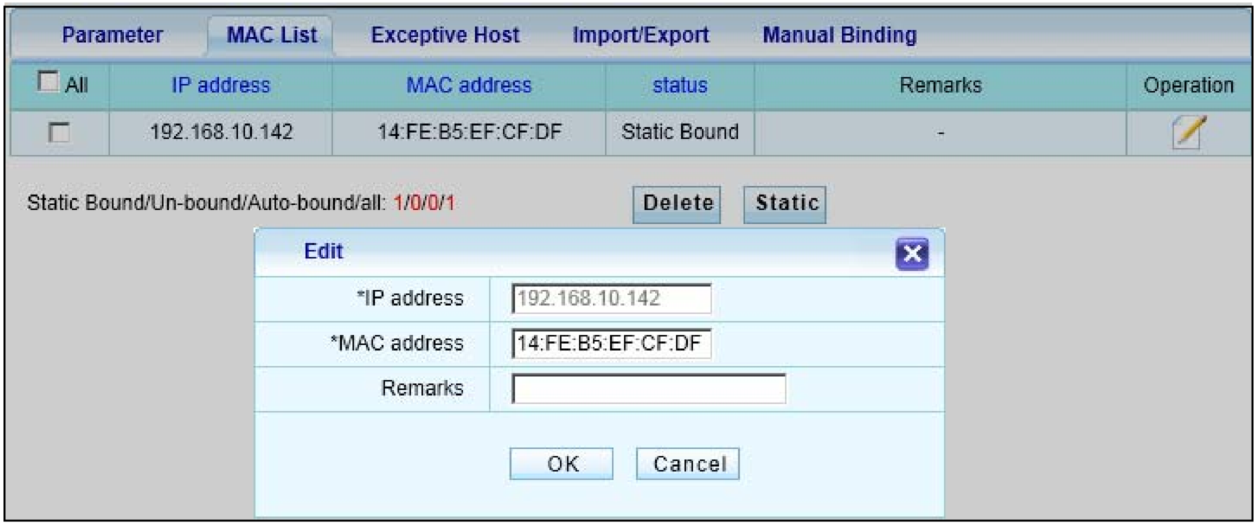
In this page you can complete IP address and specify the MAC binding/filtering rules. Open IP/MAC binding configuration page **WEB management interface -> network security ->IP with MAC bindings**, as shown below:



IP/MAC auto binding	● Enable ○ Disable
*Time	Inactive 2 Min Unbundling
Unbound prohibited	○ Enable ● Disable

(1) An unbound IP/MAC: It’s not a static binding list of IP addresses allowed through routers.

(2) Static list: Your client IP/MAC address.



□ All	IP address	MAC address	status	Remarks	Operation
□	192.168.10.142	14:FE:B5:EF:CF:DF	Static Bound	-	✎

Static Bound/Un-bound/Auto-bound/all: 1/0/0/1

*IP address	192.168.10.142
*MAC address	14:FE:B5:EF:CF:DF
Remarks	

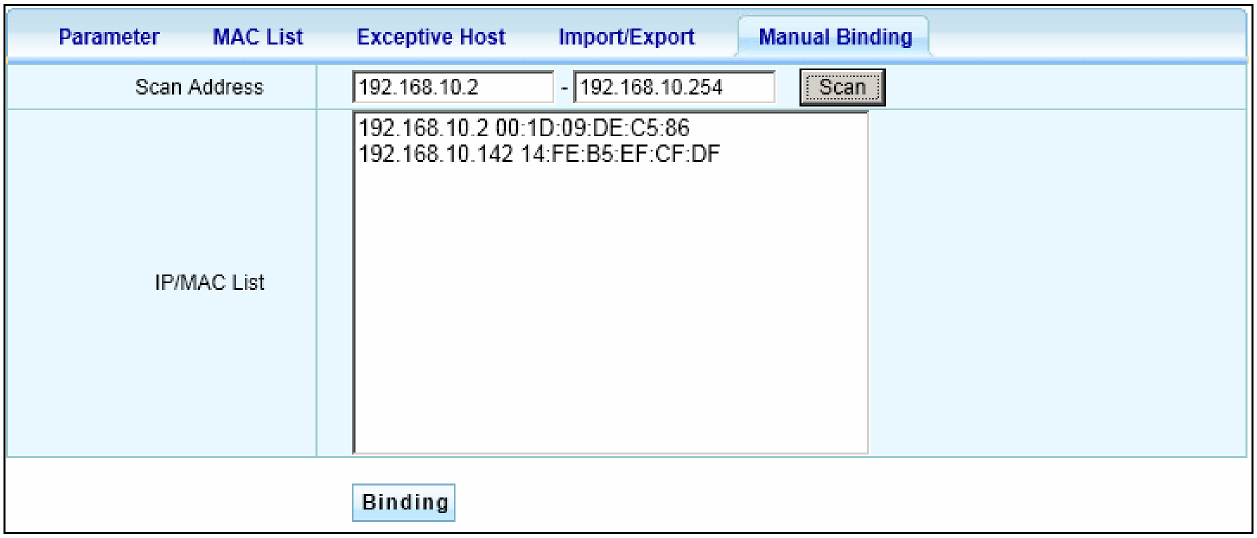
(3) IP address: Client IP addresses information.

(4) MAC address: The client MAC addresses information.

(5) Status: Client IP/MAC bound state of the address.

(6) Operation: Editable IP/MAC address binding rules, click the "**DELETE**" button to clear the

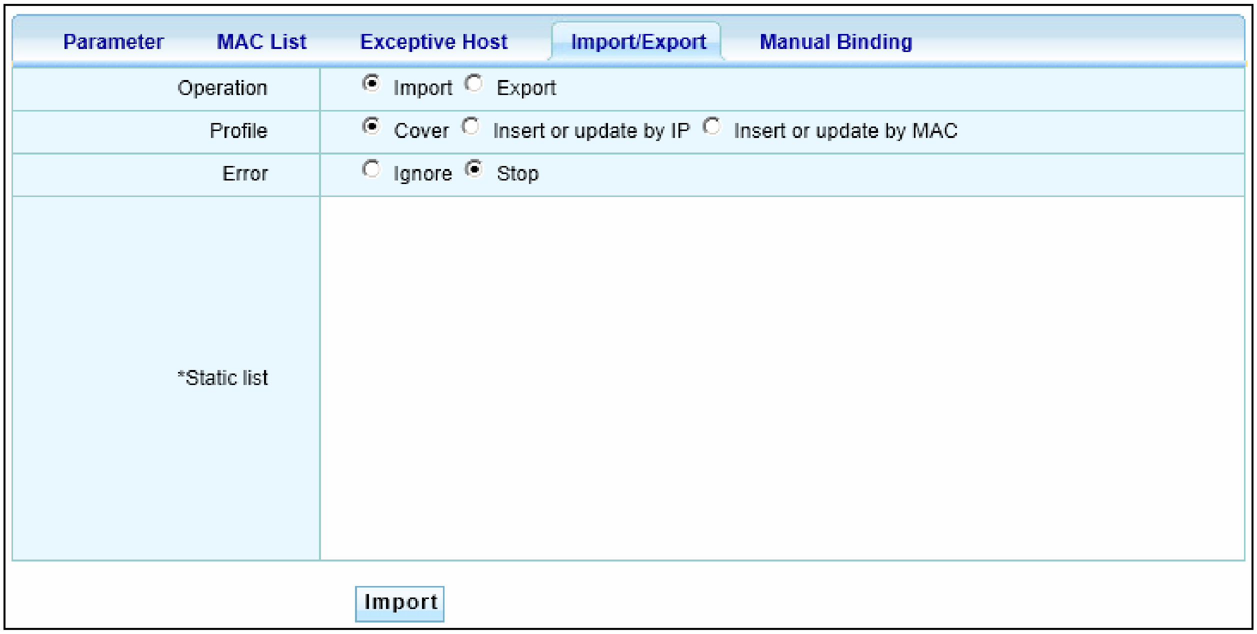
binding rule.



Scan Address	192.168.10.2 - 192.168.10.254
IP/MAC List	192.168.10.2 00:1D:09:DE:C5:86 192.168.10.142 14:FE:B5:EF:CF:DF

(9) Exceptive host: Enter the IP address of the Exceptive host.

(10) Import /Export: Import IP/MAC address list, easy to operate, as shown below:



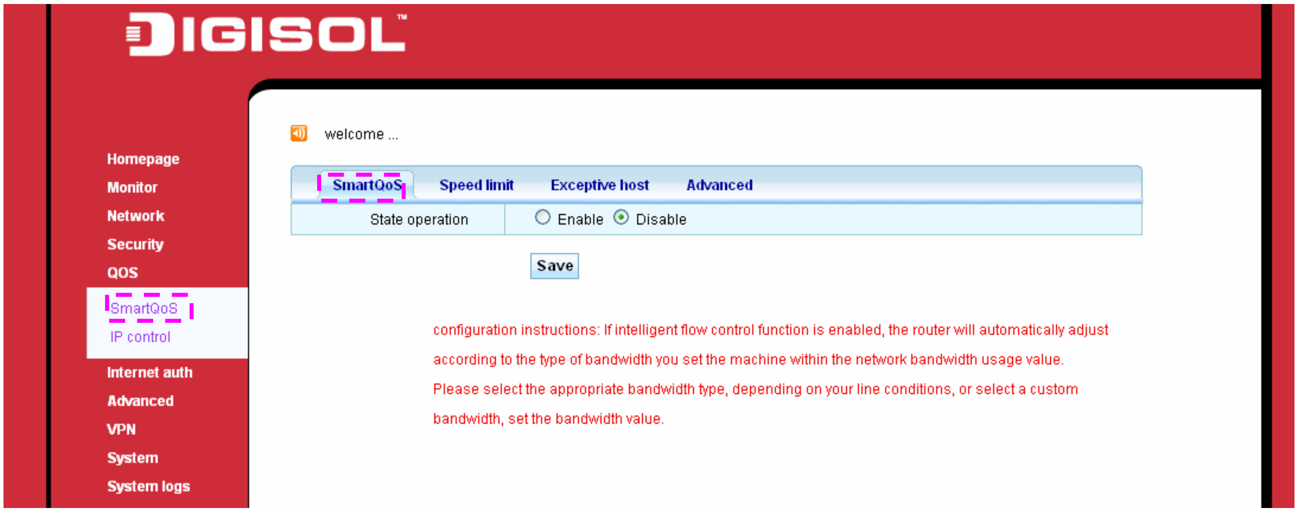
Operation	● Import ○ Export
Profile	● Cover ○ Insert or update by IP ○ Insert or update by MAC
Error	○ Ignore ● Stop
*Static list	

3.6 QoS

1. Smart QOS

In this page you can configure the up and down lines which specify the external network assigned bandwidth.

Open the intelligent flow control settings page **WEB management interface ->QOS-> SmartQoS**, as shown below:



State operation ○ Enable ● Disable

configuration instructions: If intelligent flow control function is enabled, the router will automatically adjust according to the type of bandwidth you set the machine within the network bandwidth usage value. Please select the appropriate bandwidth type, depending on your line conditions, or select a custom bandwidth, set the bandwidth value.

(1) State operation: Intelligent flow control Enable or Disable.

(2) WAN1: Select ADSL1M or fiber 2m or other forms of value, automatically fill in a predefined value, you can also choose to customize the bandwidth value, manually specify the WAN1 downlink bandwidth.

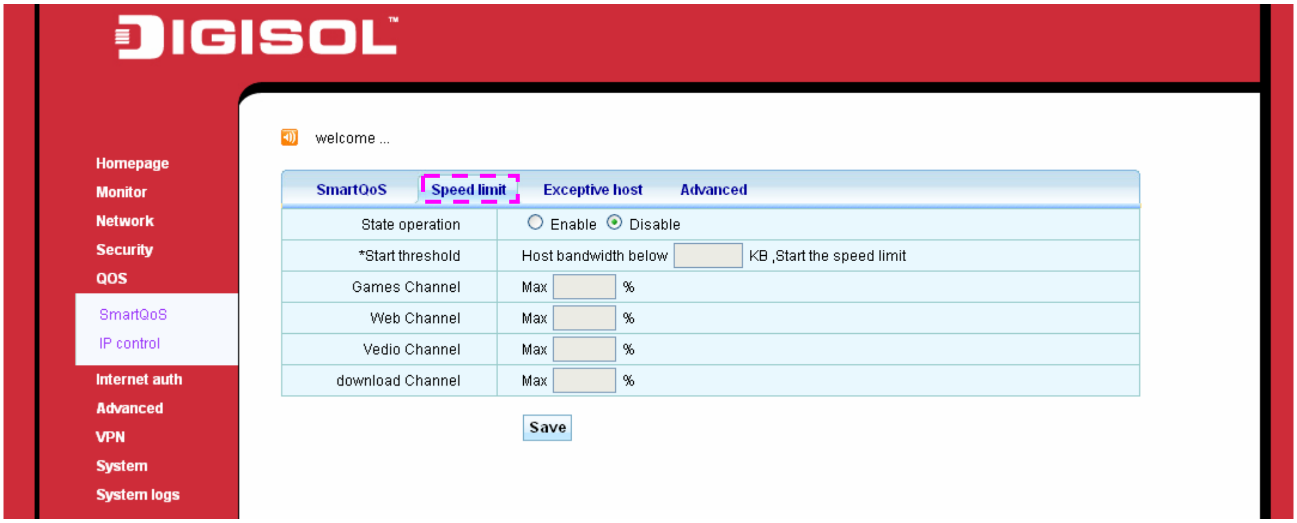
(3) WAN2: Select ADSL1M or fiber 2 m or other forms of value, automatically fill in a predefined value, you can also choose to customize the bandwidth value, manually specify the WAN2 downlink bandwidth.

(4) Save: Write the static configuration of the router, the parameters to take effect.

Speed Limit

In the configuration page, you can target a single host between different applications available bandwidth ratio, treated differently, specify the largest proportion of different applications available.

Open the channel settings page **WEB management interface ->QOS ->Speed limit**, as shown below:



State operation	○ Enable ● Disable
*Start threshold	Host bandwidth below ☐ KB ,Start the speed limit
Games Channel	Max ☐ %
Web Channel	Max ☐ %
Vedio Channel	Max ☐ %
download Channel	Max ☐ %

(1) State operations: Select whether to enable channel control.

(2) Start threshold: A single host is passive channel control threshold is enabled.

(3) Games channel: Percentage of bandwidth allocated to Games.

(4) Web channel: Percentage of bandwidth occupied by a Web application.

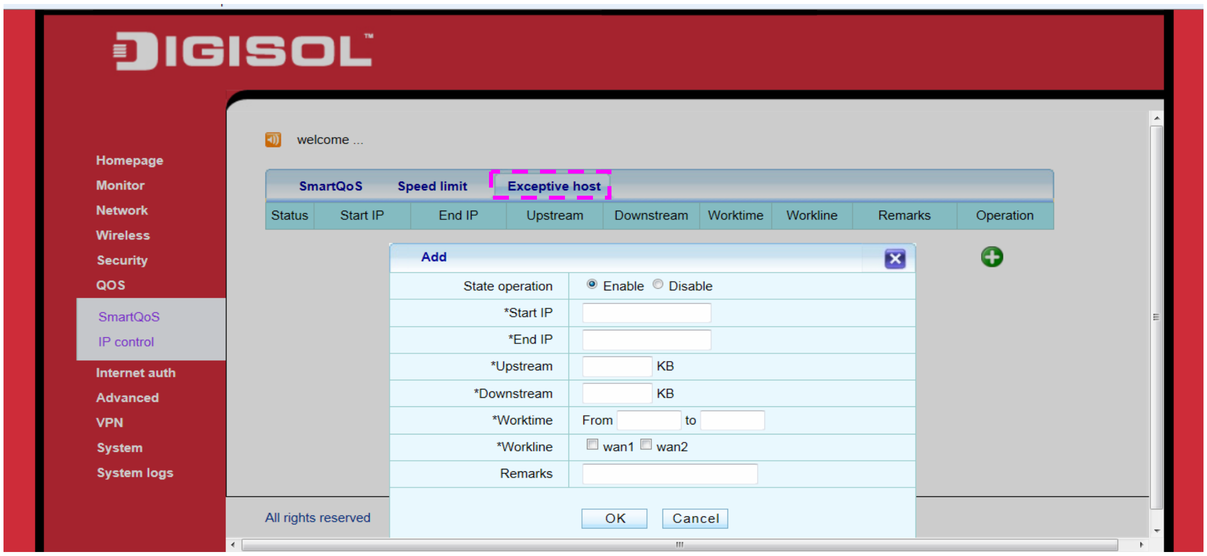
(5) Video channel: Percentage of bandwidth occupied by video

(6) Save: Write the static configuration of the router, the parameters to take effect.

Exceptive Host

Open the channel settings page **WEB management interface ->QOS-> Exceptive host**, as shown below:

Enter the IP Address range for which speed limit can be specified.



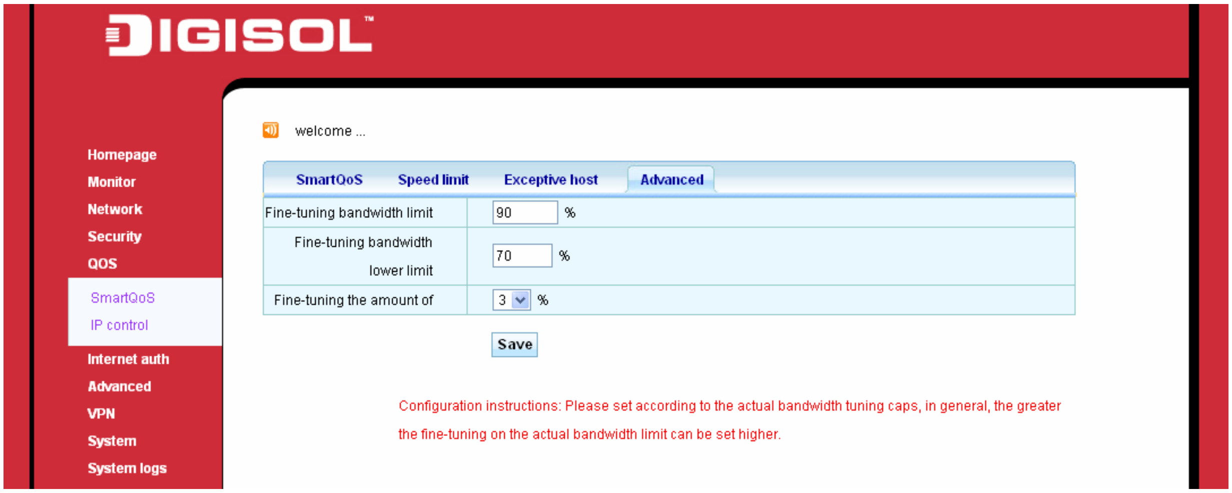
Status	Start IP	End IP	Upstream	Downstream	Worktime	Workline	Remarks	Operation

Add

State operation	● Enable ○ Disable
*Start IP	
*End IP	
*Upstream	KB
*Downstream	KB
*Worktime	From to
*Workline	□ wan1 □ wan2
Remarks	

Advanced

Open the channel settings page **WEB management interface->QOS->Advanced**, as shown below:



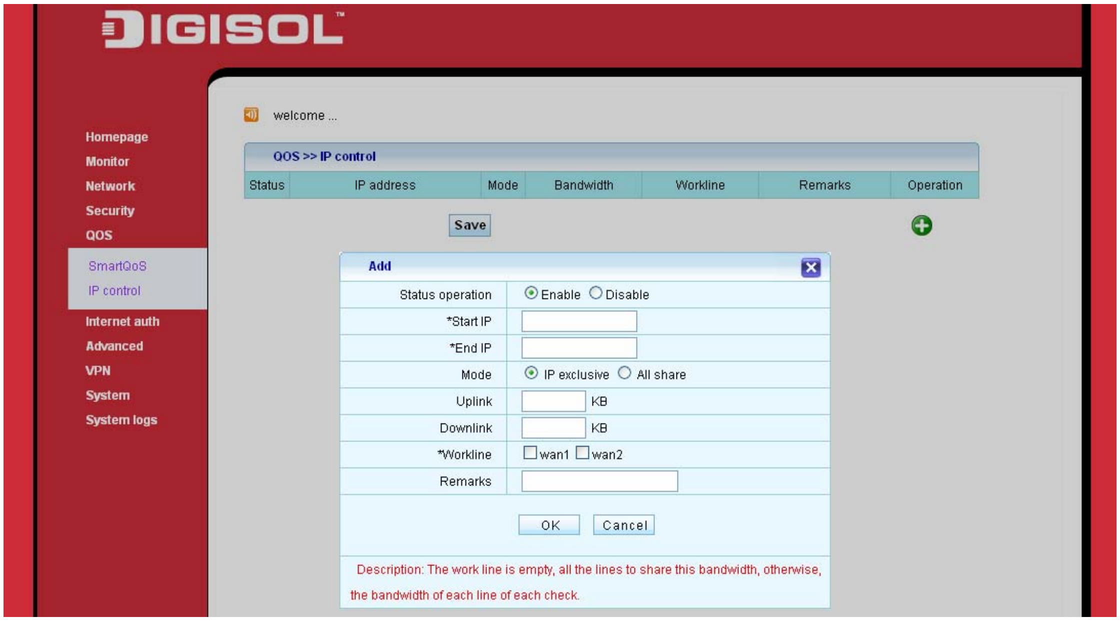
Fine-tuning bandwidth limit	90 %
Fine-tuning bandwidth lower limit	70 %
Fine-tuning the amount of	3 %

Configuration instructions: Please set according to the actual bandwidth tuning caps, in general, the greater the fine-tuning on the actual bandwidth limit can be set higher.

2. IP Control

User based or groups based internet bandwidth restrictions can be defined here. With uplink/Downlink speed defined in the specific limit, users are not allowed to cross the defined limit.

Open the channel settings page **WEB management interface->QOS->IP Filter**, as shown below:



QOS >> IP control

Status	IP address	Mode	Bandwidth	Workline	Remarks	Operation

Status operation	● Enable ○ Disable
*Start IP	
*End IP	
Mode	● IP exclusive ○ All share
Uplink	KB
Downlink	KB
*Workline	□ wan1 □ wan2
Remarks	

Description: The work line is empty, all the lines to share this bandwidth, otherwise, the bandwidth of each line of each check.

1. Status operation: Enable/Disable
2. Start IP: Starting IP address for a range of addresses.
3. End IP: End IP address for range of address. For Single user mode, defined start and end IP address as same.
4. Mode: IP Exclusive or All Shares. With IP Exclusive, each user is provided with dedicated defined bandwidth. With All share, the entire user share the defined bandwidth.
5. Uplink: bandwidth in KB.
6. Downlink: bandwidth in KB.
7. Workline: Select the Line to which rules are applicable.
8. Remark : Comment if any.

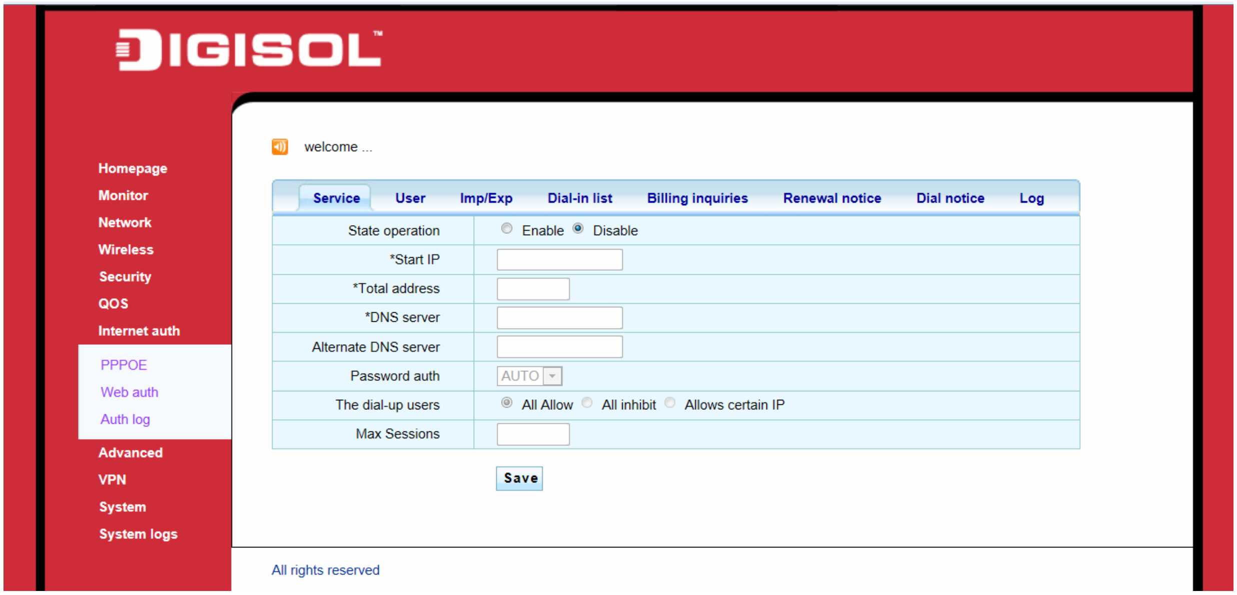
Click “**OK**” and “**Save**” the changes for settings to take effect.

3.7 Internet Authentication

3.7.1 PPPOE service

Open PPPOE service configuration page **WEB management interface ->Internet Auth ->PPPOE**.

1. Service management



State operation	○ Enable ● Disable
*Start IP	
*Total address	
*DNS server	
Alternate DNS server	
Password auth	AUTO
The dial-up users	● All Allow ○ All inhibit ○ Allows certain IP
Max Sessions	

Save

(1) State action: "Service management" function restart disabled.

(2) Start IP address: IP address of the starting IP.

(3) Total number of addresses: Allocation of IP number.

(4) DNS server: The preferred DNS Server IP address.

(5) Alternate DNS server: An alternate DNS Server IP address.

(6) Password authentication method: Used to set the password of the authentication method.

(7) The dial-up users: Select the filter users.

(8) The system maximum number of sessions: Used to set the maximum number of sessions allowed per user.

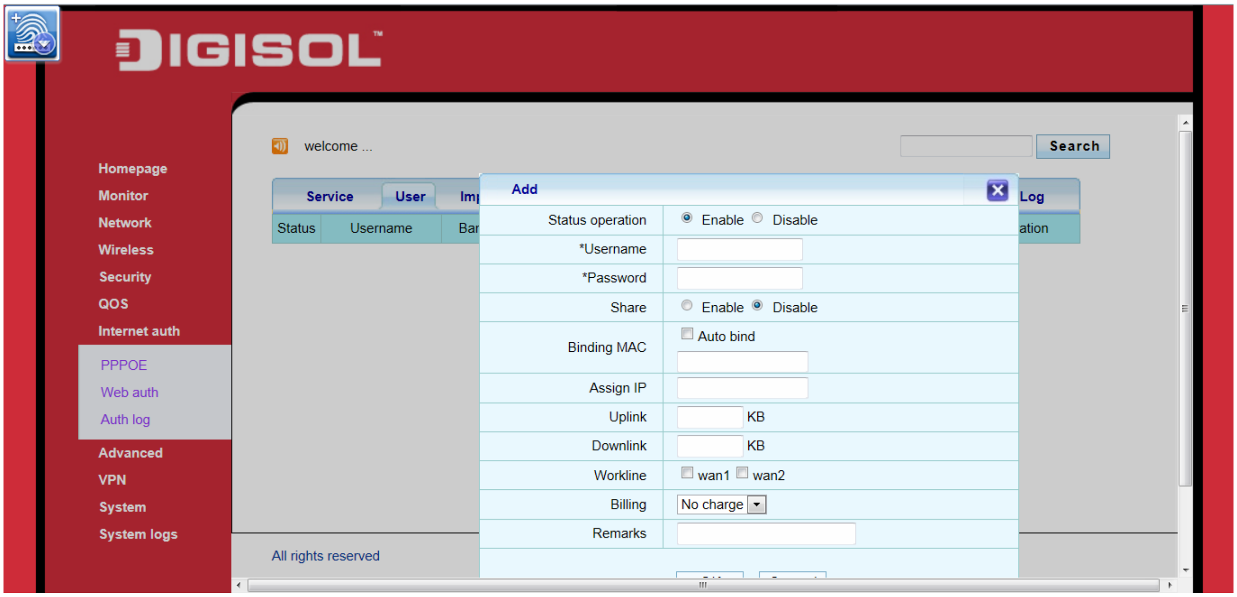
(9) Save: Write the static configuration of the router, the parameters to take effect.

Note:

(1) In this page, configure modified and saved, click on the "Save" button immediately.

(2) User management.

2. On the use of PPPoE service users to management.



Add

Status operation	● Enable ○ Disable
*Username	
*Password	
Share	○ Enable ● Disable
Binding MAC	□ Auto bind
Assign IP	
Uplink	KB
Downlink	KB
Workline	□ wan1 □ wan2
Billing	No charge
Remarks	

(1) User name: The user name of the user logged on to the system.

(2) Password: The user's login password.

(3) Share: Whether to allow multiple users to use the same account.

(4) Binding MAC: MAC address with PPPoE assigned IP address bindings

(5) Assign IP: Enter the fixed IP Address for the user.

(6) Uplink bandwidth: PPPoE users upload data bandwidth through the router

(7) Downlink bandwidth: PPPoE users download bandwidth of the data through the router

(8) Work line: PPPoE users to connect internet via Multiple WAN links

(9) Billing: Select type of billing based on Hour/time slot/flow.

(10) Save: Write the static configuration of the router, the parameters to take effect.

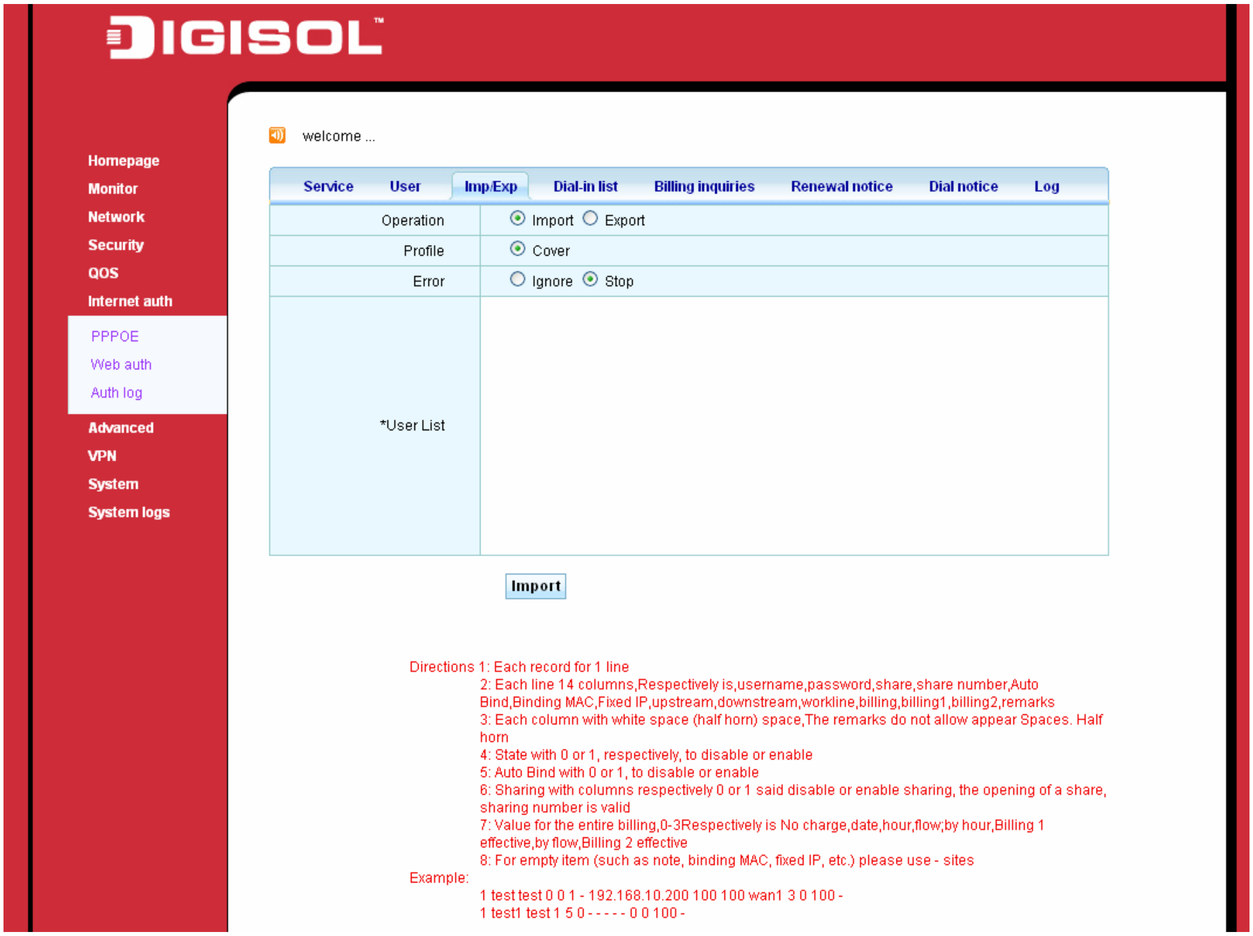
Note:

(1) In this page, configure modified and saved, click on the "Save" button to take effect immediately.

(2) " *" Identity is required.

3. Import/Export

In this page you can view PPPoE user list for import and export operations, as shown below:



Operation	● Import ○ Export
Profile	● Cover
Error	○ Ignore ● Stop
*User List	

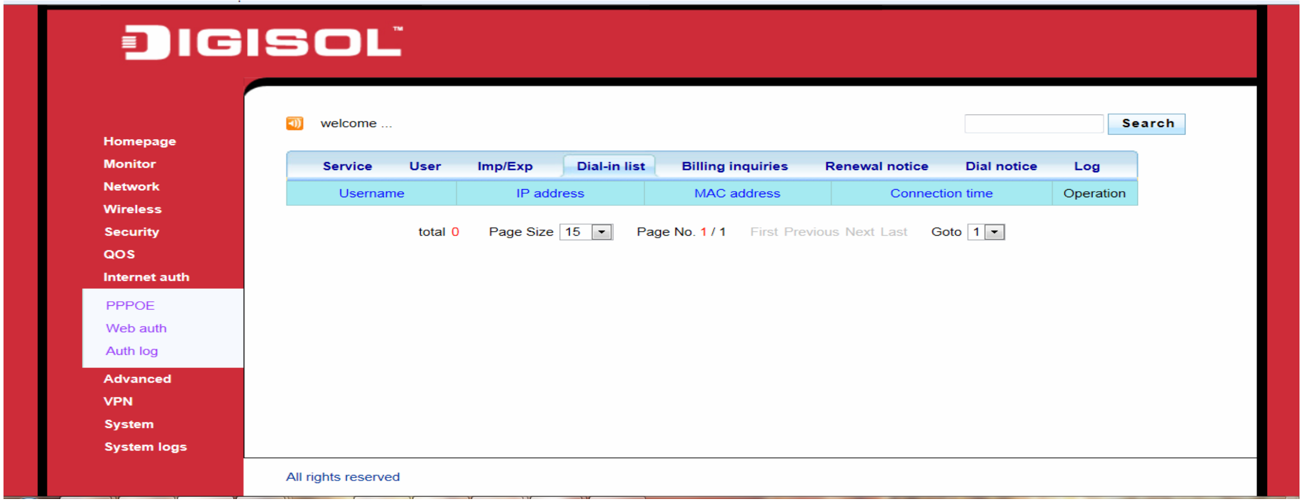
Directions 1: Each record for 1 line
2: Each line 14 columns,Respectively is,username,password,share,share number,Auto Bind,Binding MAC,Fixed IP,upstream,downstream,workline,billing,billing1,billing2,remarks
3: Each column with white space (half horn) space,The remarks do not allow appear Spaces. Half horn
4: State with 0 or 1, respectively, to disable or enable
5: Auto Bind with 0 or 1, to disable or enable
6: Sharing with columns respectively 0 or 1 said disable or enable sharing, the opening of a share, sharing number is valid
7: Value for the entire billing,0-3Respectively is No charge,date,hour,flow;by hour,Billing 1 effective,by flow,Billing 2 effective
8: For empty item (such as note, binding MAC, fixed IP, etc.) please use - sites

Example:

```
1 test test 0 0 1 - 192.168.10.200 100 100 wan1 3 0 100 -
1 test1 test 1 5 0 - - - - - 0 0 100 -
```

4. dial-in list

In this page you can view using PPPOE dial routing user list, as shown below:



Username	IP address	MAC address	Connection time	Operation

total 0 Page Size 15 Page No. 1 / 1 First Previous Next Last Goto 1

(1) User name: PPPoE user name of the account.

(2) IP address: User host access to IP addresses.

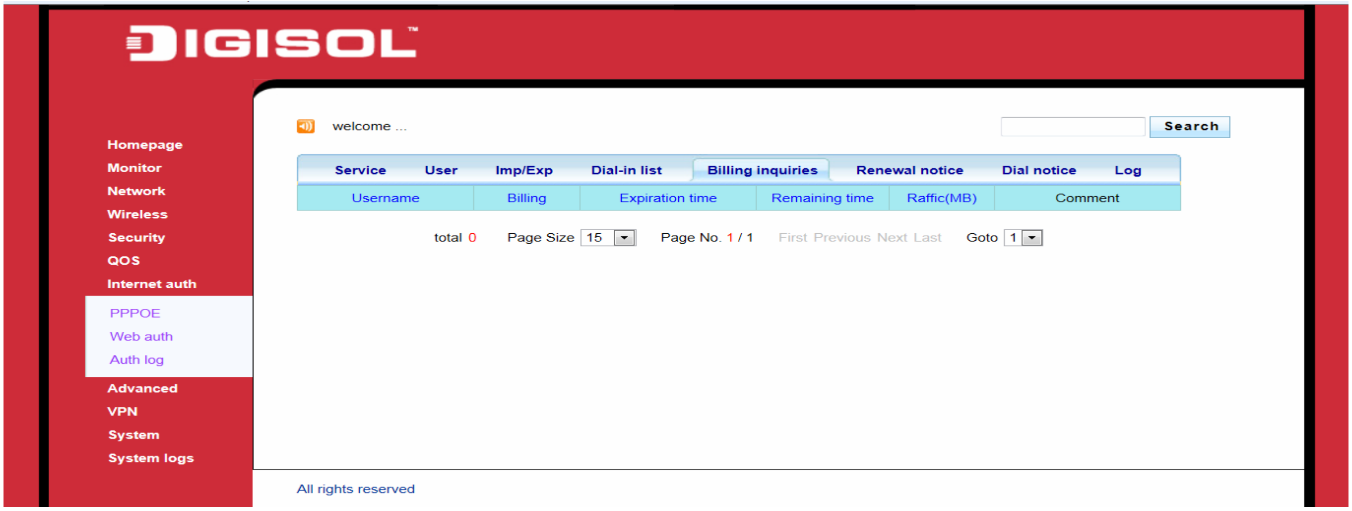
(3) MAC address: User host network adapter physical address.

(4) Connect time: User’s online connection time.

(5) Action: Can be specified manually, PPPOE user.

5. Billing inquiries

In this page you can view the open billing PPPoE user billing status, as shown below.



Username	Billing	Expiration time	Remaining time	Raffic(MB)	Comment

total 0 Page Size 15 Page No. 1 / 1 Goto 1

(1) User name: PPPoE user name of the account.

(2) Billing: Billing of accounts.

(3) Expiration time: PPPOE account expiration time.

(4) Remaining Time: PPPOE accounts rest time

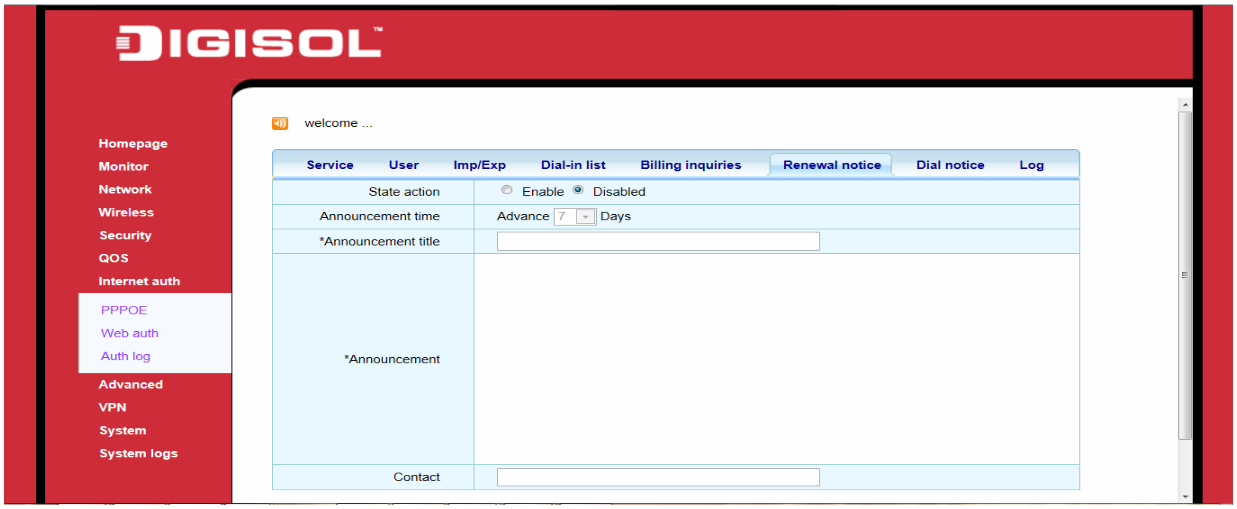
(5) Save: Write the static configuration of the router, the parameters to take effect.

Note:

(1) In this page, according to the different billing method, expiration time, remaining time and the remaining flow three features, display and will not display time.

6. The renewal notice

In this page on the net PPPoE users will get an Expiration notice as configured below to remind the user to renew in time.



State action	○ Enable ● Disabled
Announcement time	Advance 7 Days
*Announcement title	
*Announcement	
Contact	

(1) State action: Renew bulletin features enabled and disabled state.

(2) Announcement time: User received in advance PPPoE notice time period.

(3) Announcement title: Title of the renewal notice.

(4) Announcement: Details of the renewal notice.

(5) Contact: Fill in the Administrator's contact, easy renewals in a timely manner.

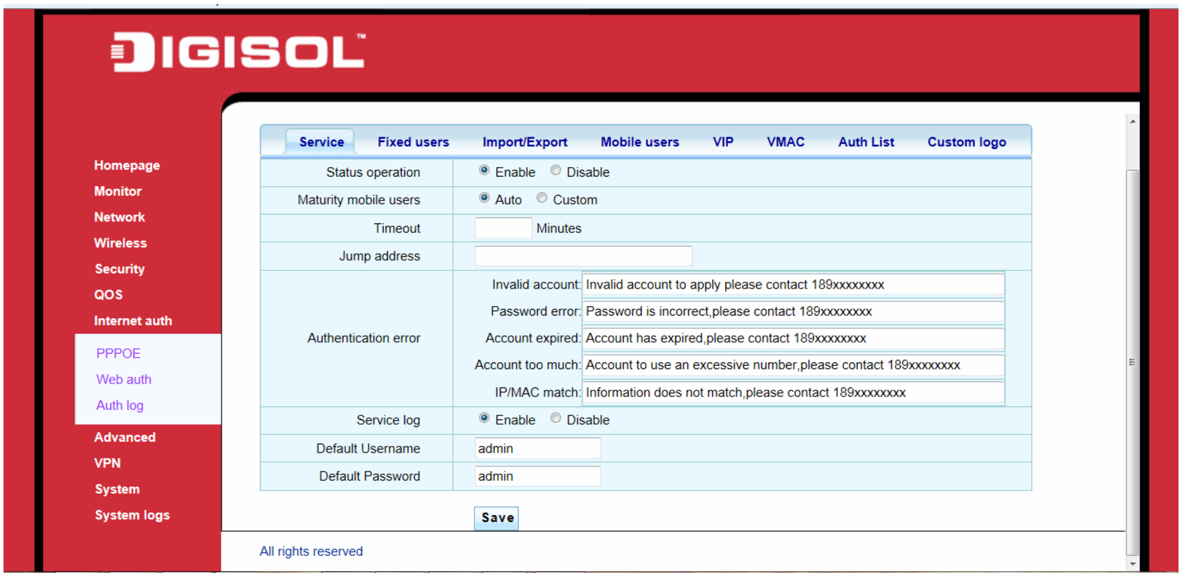
(6) Preview: Preview the bulletin content published to the user; see if there is an error.

(7) Save: Write the static configuration of the router, the parameters to take effect.

3.7.2 WEB authentication

1. Service configuration

In the configuration page, you can configure WEB authentication capabilities,

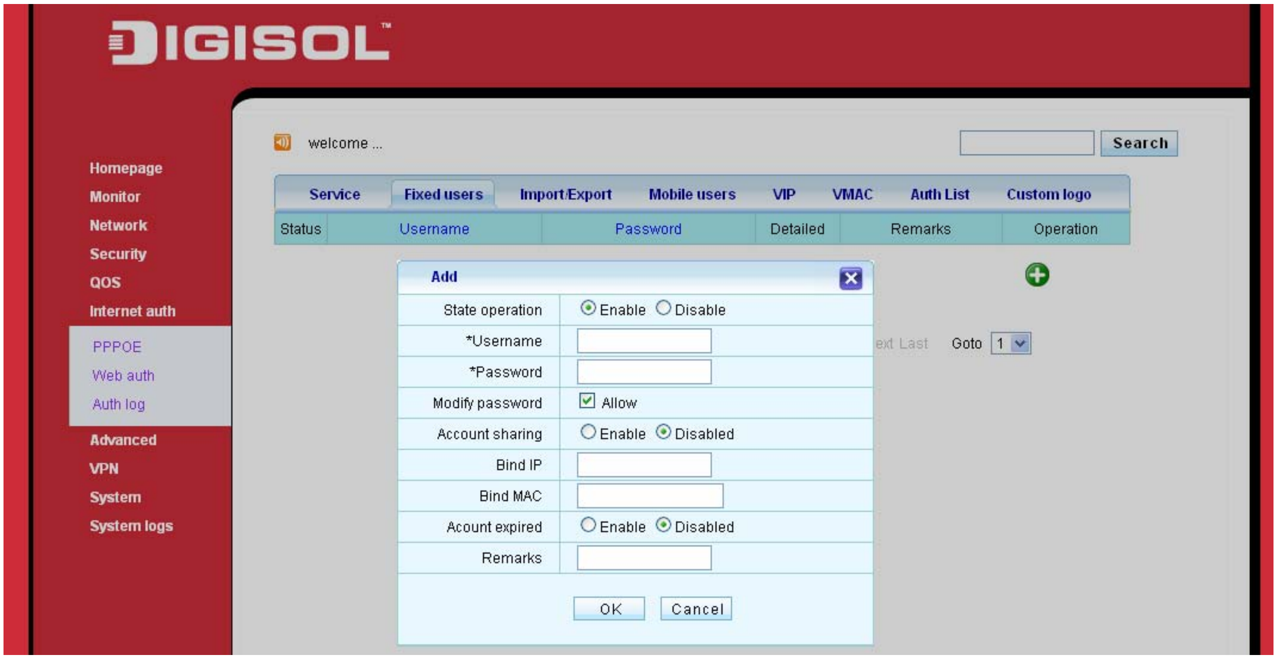


Status operation	● Enable ○ Disable	
Maturity mobile users	● Auto ○ Custom	
Timeout	Minutes	
Jump address		
Authentication error	Invalid account:	Invalid account to apply please contact 189xxxxxxxx
	Password error:	Password is incorrect,please contact 189xxxxxxxx
	Account expired:	Account has expired,please contact 189xxxxxxxx
	Account too much:	Account to use an excessive number,please contact 189xxxxxxxx
	IP/MAC match:	Information does not match,please contact 189xxxxxxxx
Service log	● Enable ○ Disable	
Default Username	admin	
Default Password	admin	

(1) Status operation: Select Enable or Disable WEB authentication capabilities.
(2) Maturity mobile users: There are two options: Auto and Custom.
(3) Timeout: Routing authentication when users exceed this time is detected, this user is automatically logged off.
(4) Jump address: You can manually enter the user authentication page fill in the user name and password, and then jump to Web site.
(5) Authentication error: Appears when the user account is invalid, wrong password etc.
(6) Service log: WEB authentication service log is enabled or disabled.
(7) Default Username/Password: Enter default username/password that will appear on the Web auth login window
(8) Save: Write the static configuration of the router, the parameters to take effect.

2. Fixed user

In the configuration page, you can configure the login WEB authentication feature fixed account, as shown:

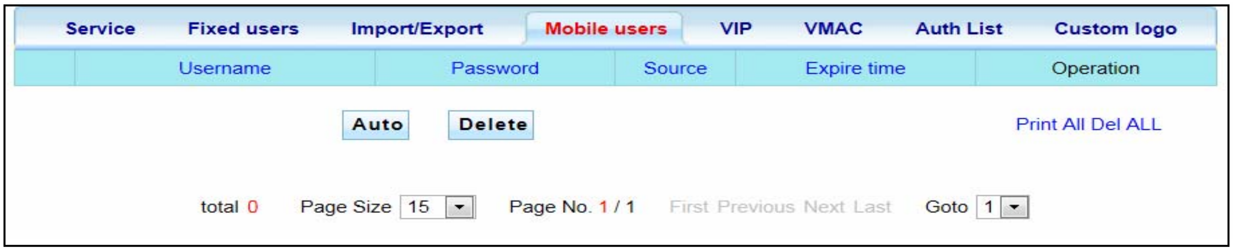


State operation	● Enable ○ Disable
*Username	
*Password	
Modify password	☑ Allow
Account sharing	○ Enable ● Disabled
Bind IP	
Bind MAC	
Acount expired	○ Enable ● Disabled
Remarks	

(1) Status: Fixed user chooses whether to enable or disable the current configuration.
(2) User name: User login WEB authentication of the user name.
(3) Password: Login WEB authentication password.
(4) Account sharing: Whether to allow multiple users to use the same account restart disabled.
(5) Bind IP: Enter the fixed account you want to bind the client IP address, after binding, other client computers cannot use this account.
(6) Bind MAC: Insert into the fixed accounts you want to bind the client MAC address, after binding, other client computers cannot use this account.
(7) Account expired: Select enable disable current account will expire.
(8) Save: Write the static configuration of the router, the parameters to take effect.

3. Mobile users

In the configuration page, you can do this by routing, automatic generation of landing WEB authentication flow accounts for internal movement of personnel management for your convenience, as shown below:



	Username	Password	Source	Expire time	Operation

(1) Generated automatically (Auto): click on the automatically generated function, you can choose to build mobile account number and expiration date.

(2) Delete expired: Automatically delete expired accounts.

(3) User name: Mobile user generated user names.

(4) Password: Generates mobile user password.

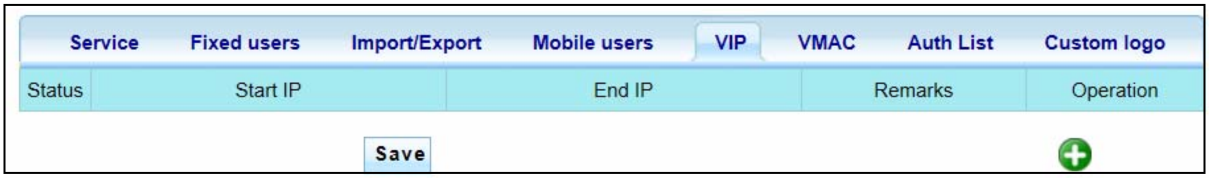
(5) Source: Locally generated mobile database.

(6) Expire Time: This mobile account expiration Time.

(7) Action: You can print and copy the mobile account, and so on.

4. VIP (Exception IP)

In the configuration page, you can set up against WEB authentication restrictions (exceptions to IP addresses) as shown below:



Status	Start IP	End IP	Remarks	Operation

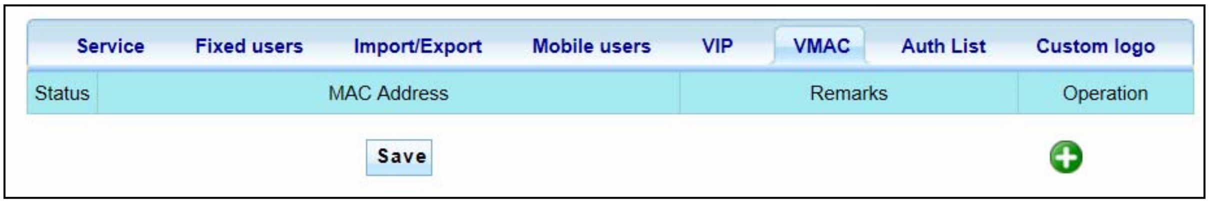
(1) Status operation: Select Enable or disable the current exception IP rules.

(2) Start IP: Enter Starting Address of Exception IP Address range.

(3) End IP: Enter End Address of Exception IP Address range.

5. VMAC (Exception MAC)

In the configuration page, you can set up against WEB authentication capabilities limited exception of MAC addresses, as shown below:



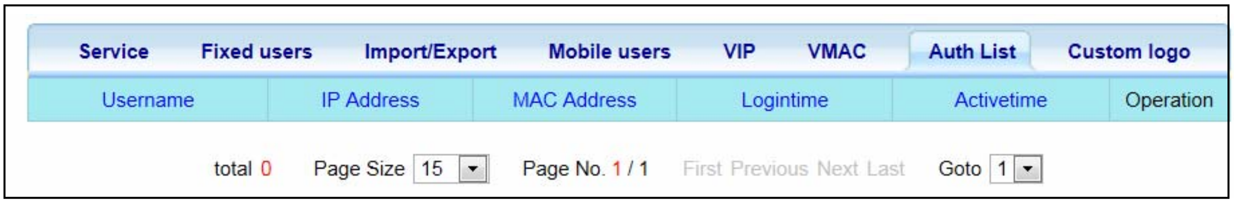
Status	MAC Address	Remarks	Operation

(1) Status operations: Select Enable or disable the current exception MAC rules.

(2) MAC address: Enter VIP MAC addresses.

6. Auth list

In the configuration page, you can view the authentication among hosts for more information, as shown below:



Username	IP Address	MAC Address	Logintime	Activetime	Operation

total 0 Page Size 15 Page No. 1 / 1 Goto 1

(1) User name: Certified users WEB authentication accounts.

(2) IP address: Authenticated user IP address information.

(3) MAC address: Authenticate users MAC address information.

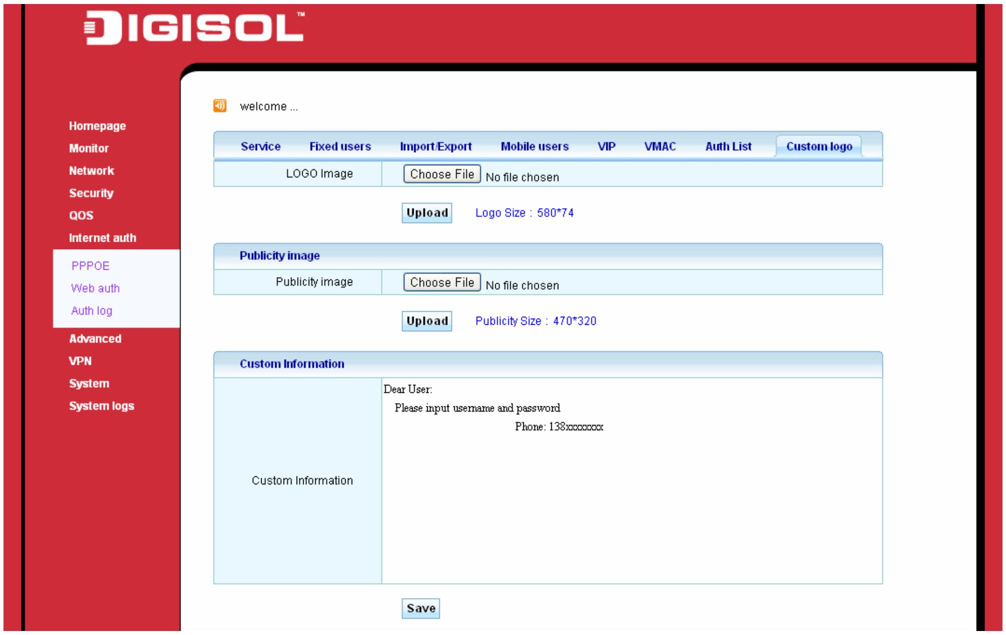
(4) Login time: Users last authentication time.

(5) Active time: Current running time.

(6) Operation: You can manually unregister this authentication user.

7. Custom Logo

With Web authentication enabled, user is promoted with the authentication page when trying to access the internet or network resources. The default page can be customized by modifying web page content which includes Logo, publicity image and login text.



LOGO Image: Choose File No file chosen

Logo Size : 580*74

Publicity image: Choose File No file chosen

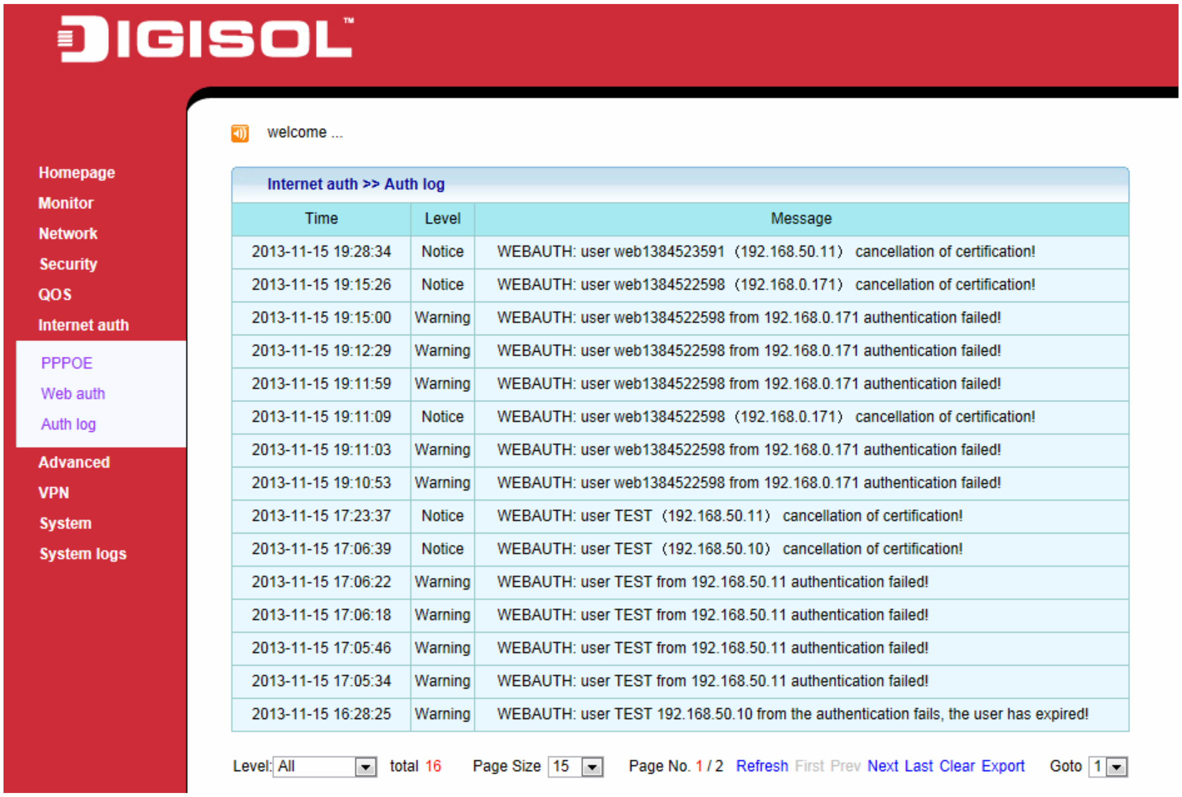
Publicity Size : 470*320

Custom Information:

Dear User:
Please input username and password
Phone: 138xxxxxxxx

3.7.3 Authentication Log

This window displays warning, notification messages related to Web Auth and PPPOE.



Internet auth >> Auth log

Time	Level	Message
2013-11-15 19:28:34	Notice	WEBAUTH: user web1384523591（192.168.50.11） cancellation of certification!
2013-11-15 19:15:26	Notice	WEBAUTH: user web1384522598（192.168.0.171） cancellation of certification!
2013-11-15 19:15:00	Warning	WEBAUTH: user web1384522598 from 192.168.0.171 authentication failed!
2013-11-15 19:12:29	Warning	WEBAUTH: user web1384522598 from 192.168.0.171 authentication failed!
2013-11-15 19:11:59	Warning	WEBAUTH: user web1384522598 from 192.168.0.171 authentication failed!
2013-11-15 19:11:09	Notice	WEBAUTH: user web1384522598（192.168.0.171） cancellation of certification!
2013-11-15 19:11:03	Warning	WEBAUTH: user web1384522598 from 192.168.0.171 authentication failed!
2013-11-15 19:10:53	Warning	WEBAUTH: user web1384522598 from 192.168.0.171 authentication failed!
2013-11-15 17:23:37	Notice	WEBAUTH: user TEST（192.168.50.11） cancellation of certification!
2013-11-15 17:06:39	Notice	WEBAUTH: user TEST（192.168.50.10） cancellation of certification!
2013-11-15 17:06:22	Warning	WEBAUTH: user TEST from 192.168.50.11 authentication failed!
2013-11-15 17:06:18	Warning	WEBAUTH: user TEST from 192.168.50.11 authentication failed!
2013-11-15 17:05:46	Warning	WEBAUTH: user TEST from 192.168.50.11 authentication failed!
2013-11-15 17:05:34	Warning	WEBAUTH: user TEST from 192.168.50.11 authentication failed!
2013-11-15 16:28:25	Warning	WEBAUTH: user TEST 192.168.50.10 from the authentication fails, the user has expired!

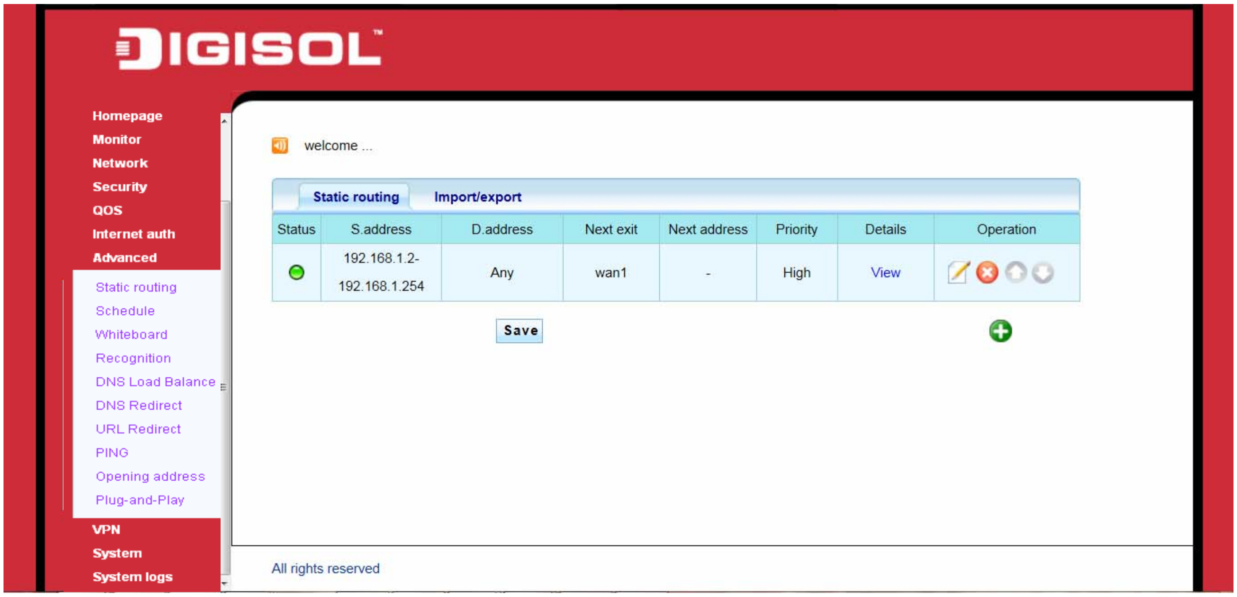
Level: All total 16 Page Size 15 Page No. 1 / 2 Refresh First Prev Next Last Clear Export Goto 1

3.8 Advanced Configuration

3.8.1 Static Routing

In the configuration page, you can configure static routing, which manually specify a network access to the path. Static routing features determine the course of data flows on your network.

Open the static route configuration page **WEB management interface -> Advanced Configuration -> static routing**, as shown below:



Status	S.address	D.address	Next exit	Next address	Priority	Details	Operation
●	192.168.1.2- 192.168.1.254	Any	wan1	-	High	View	

(1) Status operation: Select to enable or disable static routing rules.

(2) S addr: Source (LAN) start network address

(3) D addr: Source (LAN) end network address

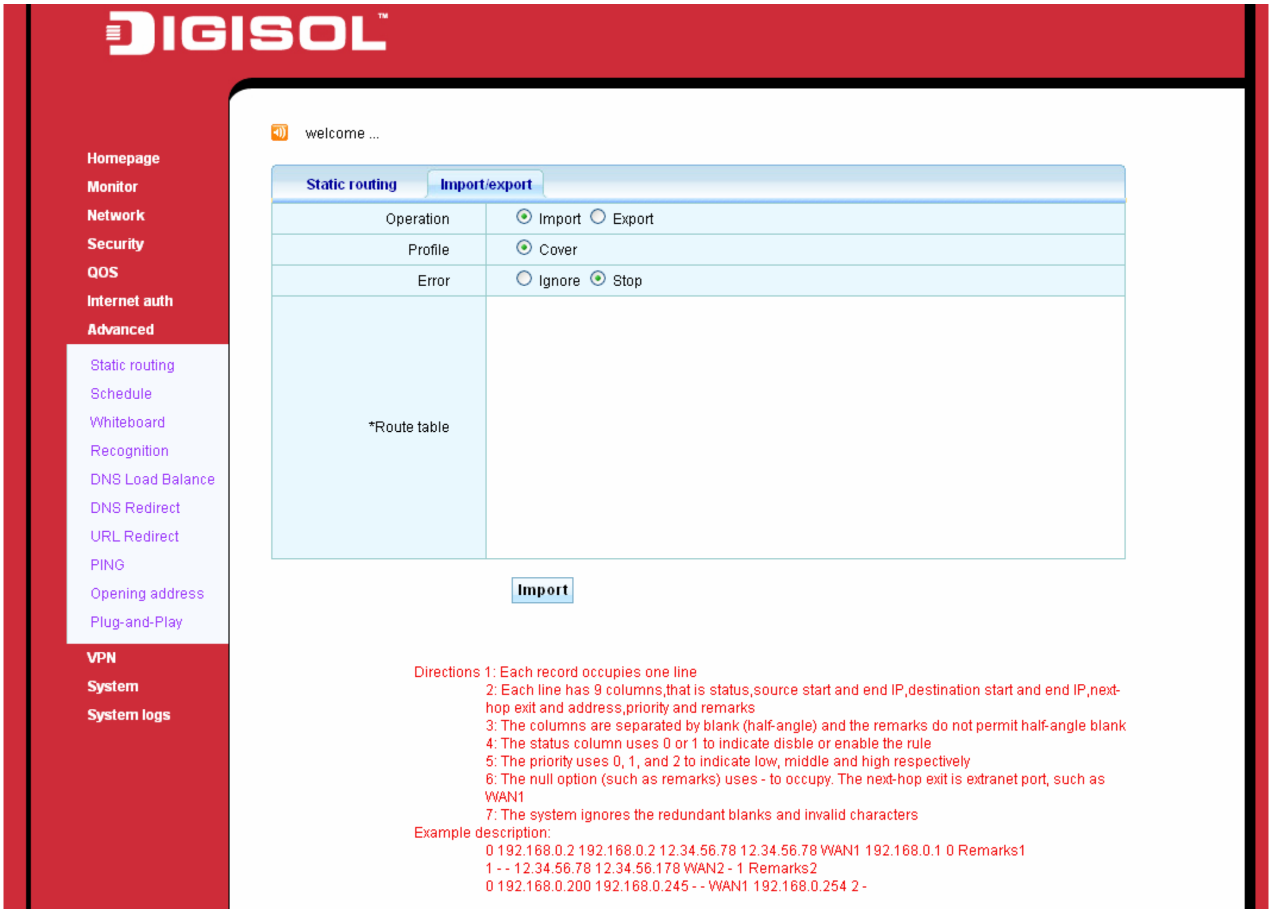
(4) Next hop address: Data goes at the destination network to go through to the next node.

(5) Priority: Priority.

(6) Save: Write the static configuration of the router, the parameters to take effect.

Import/Export

Static routes can be added on rule by rule basis using a “**static routing**” tab. For large network deployment, multiple routes can be imported at once using Import/Export Tab. Refer following consideration for rules import.



Operation	● Import ○ Export
Profile	● Cover
Error	○ Ignore ● Stop
*Route table	

Directions 1: Each record occupies one line
2: Each line has 9 columns,that is status,source start and end IP,destination start and end IP,next-hop exit and address,priority and remarks
3: The columns are separated by blank (half-angle) and the remarks do not permit half-angle blank
4: The status column uses 0 or 1 to indicate disble or enable the rule
5: The priority uses 0, 1, and 2 to indicate low, middle and high respectively
6: The null option (such as remarks) uses - to occupy. The next-hop exit is extranet port, such as WAN1
7: The system ignores the redundant blanks and invalid characters

Example description:

```
0 192.168.0.2 192.168.0.2 12.34.56.78 12.34.56.78 WAN1 192.168.0.1 0 Remarks1
1 - - 12.34.56.78 12.34.56.178 WAN2 - 1 Remarks2
0 192.168.0.200 192.168.0.245 - - WAN1 192.168.0.254 2 -
```

Configuration Consideration:

1. Each record occupies one line.
2. Each line has 9 columns, that is status, source start and end IP, destination start and end IP, next-hop exit and address, priority and remarks.
3. The columns are separated by blank (half-angle) and the remarks do not permit half-angle blank
4. The status column uses 0 or 1 to indicate disable or enable the rule.
5. The priority uses 0, 1, and 2 to indicate low, middle and high respectively.

6. The null option (such as remarks) uses - to occupy. The next-hop exit is extranet port, such as WAN1.

Example:

0 192.168.0.2 192.168.0.2 12.34.56.78 12.34.56.78 WAN1 192.168.0.1 0 Remarks1

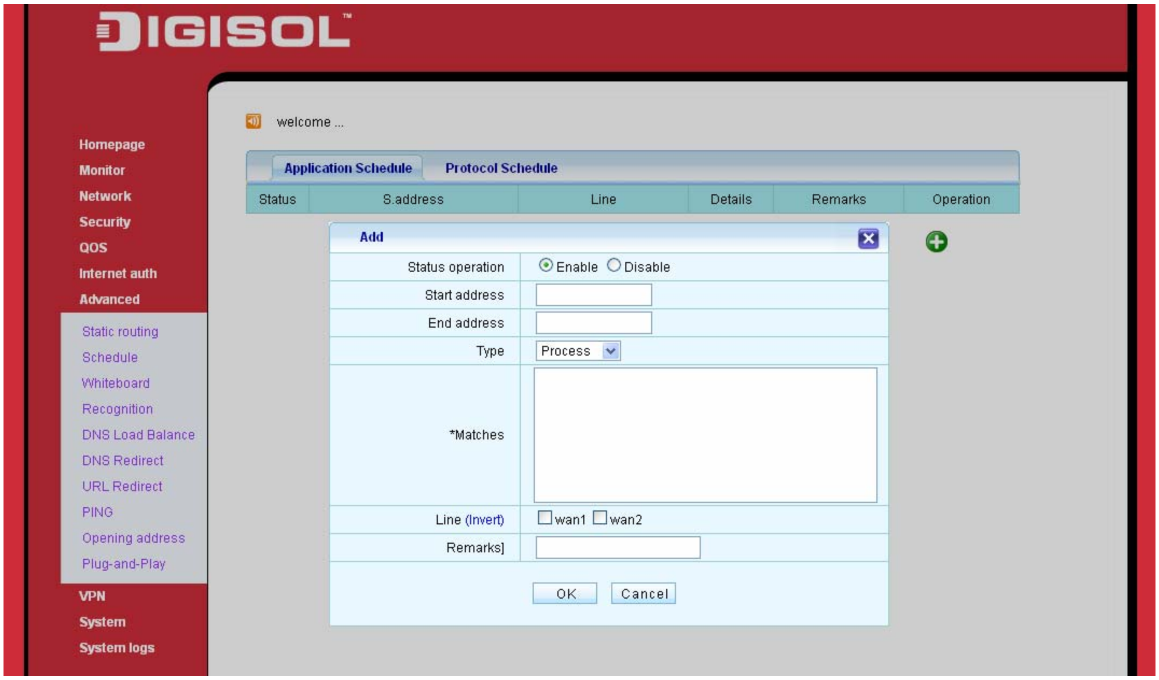
Once the routes are added in the routing table, they can be listed for review using Export tab.

3.8.2 Schedule

With Schedule option, user traffic can be matched based on application/protocol information and can be diverted to Defined WAN interface.

Application Schedule: Application specific traffic like E-mail, online games, chat etc. can be defined in this tab.

Protocol Schedule: Define traffic based on TCP/UDP port information.



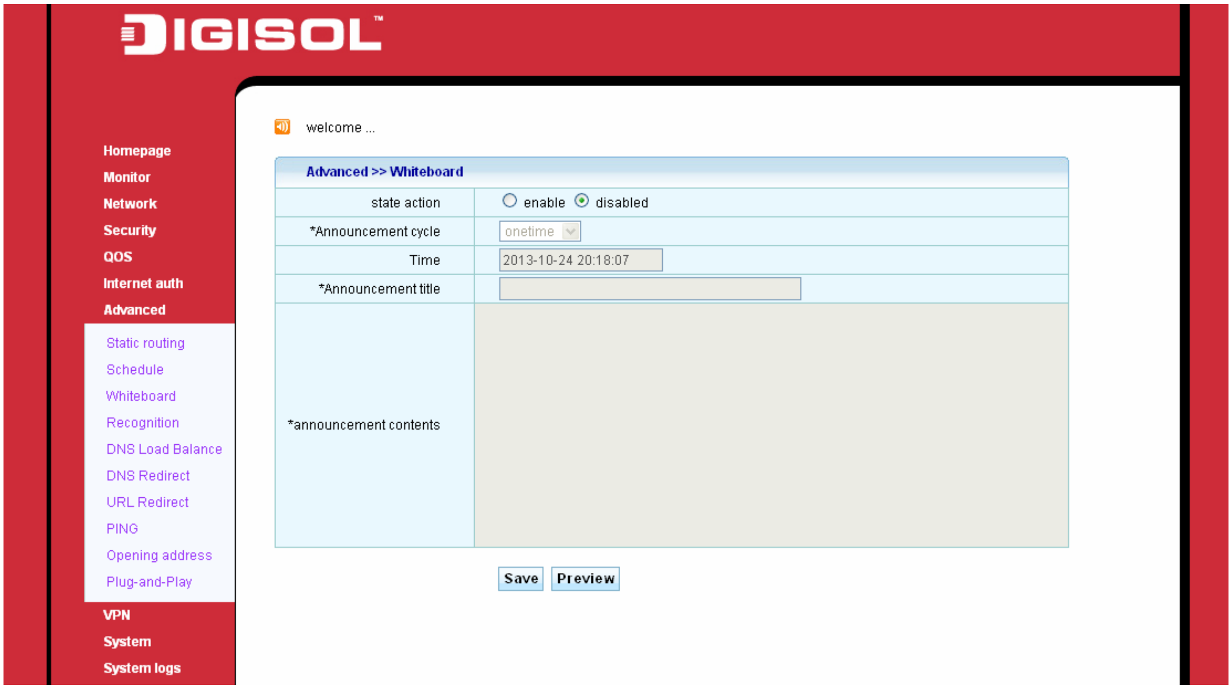
Status	S.address	Line	Details	Remarks	Operation

Status operation	● Enable ○ Disable
Start address	
End address	
Type	Process
*Matches	
Line (Invert)	□ wan1 □ wan2
Remarks]	

3.8.3 Whiteboard

Administration can make on-demand or scheduled based notifications to end user. Announcement are customization and can include information related to Network Downtimes, policy modification etc.

Announcements can be made onetime, daily basis or at more customized time using custom option.

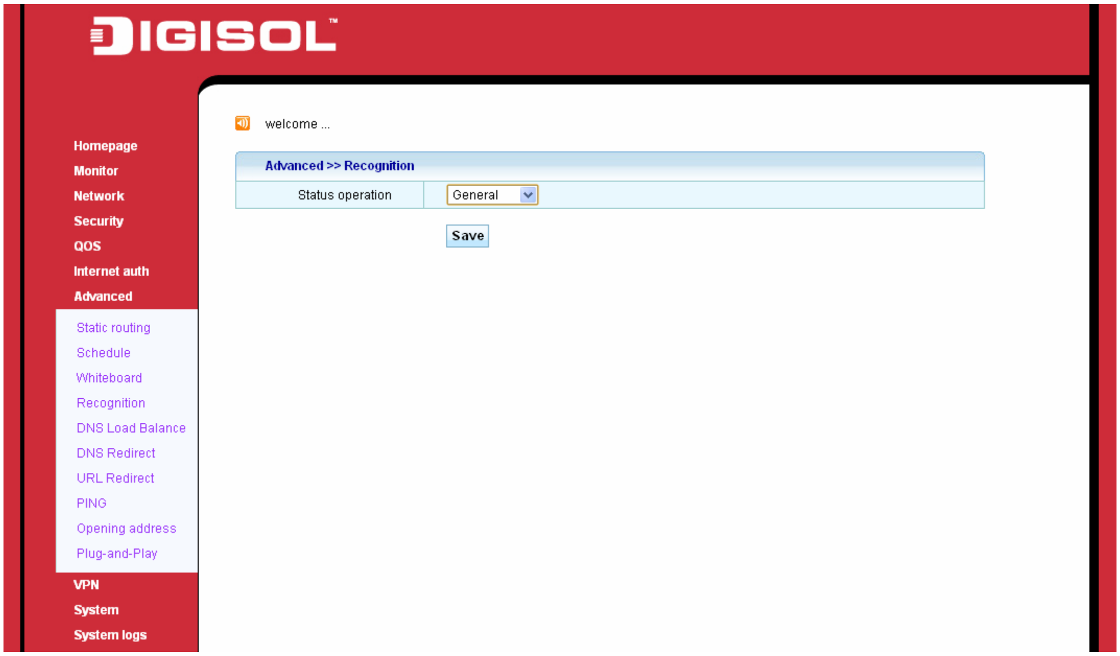


welcome ...

Advanced >> Whiteboard

state action	○ enable ● disabled
*Announcement cycle	onetime
Time	2013-10-24 20:18:07
*Announcement title	
*announcement contents	

3.8.4 Recognition

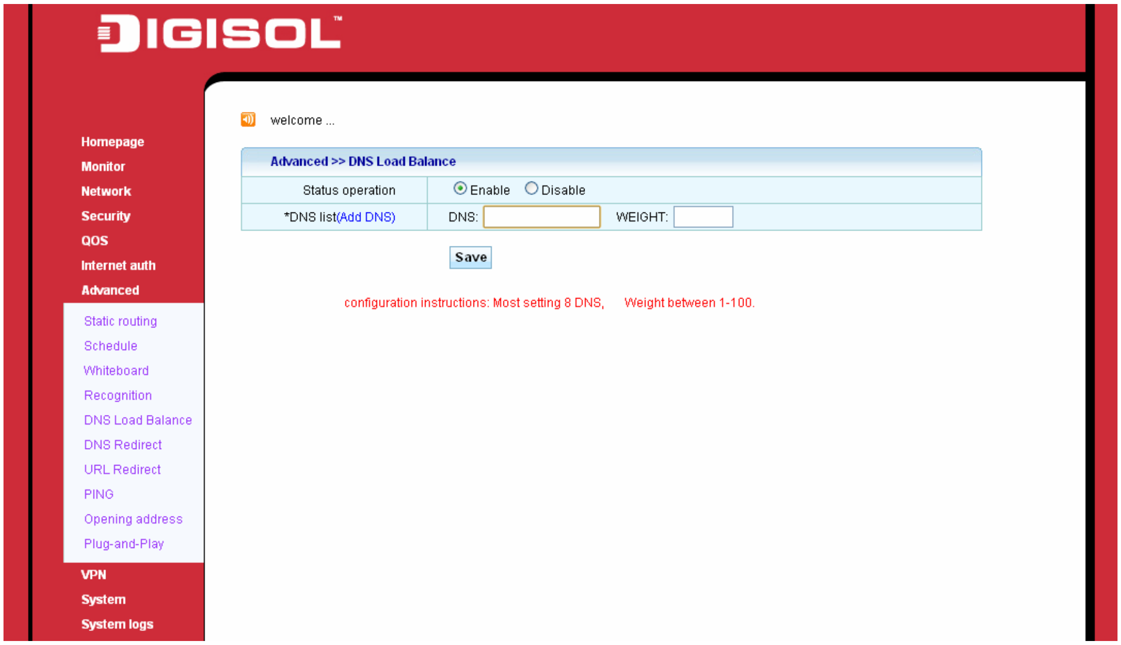


Advanced >> Recognition

Status operation: General

3.8.5 DNS Load Balance

When there are multiple DNS servers hosted in network, this tab can be used to distribute the DNS resolution load among defined servers. Up to 8 server can be defined in the table below with service weight varying from 1-100. Open the static route configuration page **WEB management interface -> Advanced Configuration -> DNS Load Balance**, as shown below:



Advanced >> DNS Load Balance

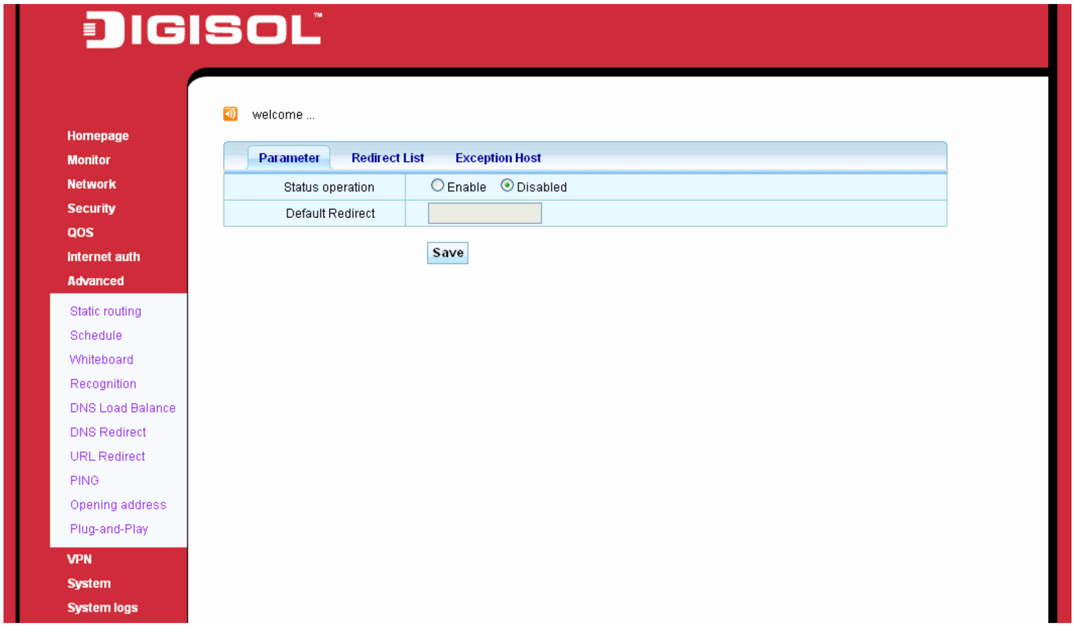
Status operation	● Enable ○ Disable
*DNS list(Add DNS)	DNS: ▭ WEIGHT: ▭

configuration instructions: Most setting 8 DNS, Weight between 1-100.

3.8.6 DNS Redirect/URL Redirect

DNS or URL rules for redirection can be defined in these tabs. When user tries to resolve/access a specific domain/URL, router diverts a request to defined DNS server/URL based on match list.

Users can be added to exception list so that the defined set of rules won't be application for specific users.

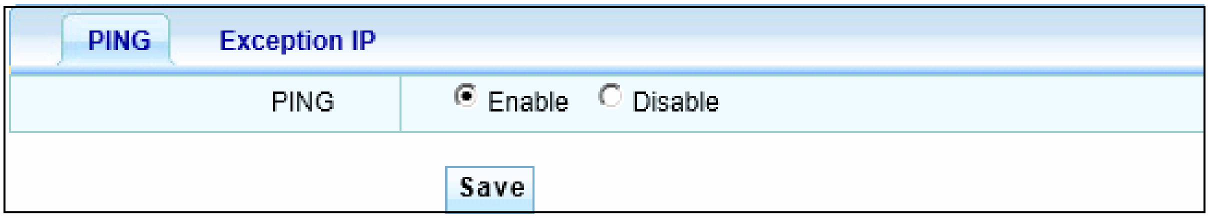


Status operation	○ Enable ● Disabled
Default Redirect	

3.8.7 PING

1. PING forced

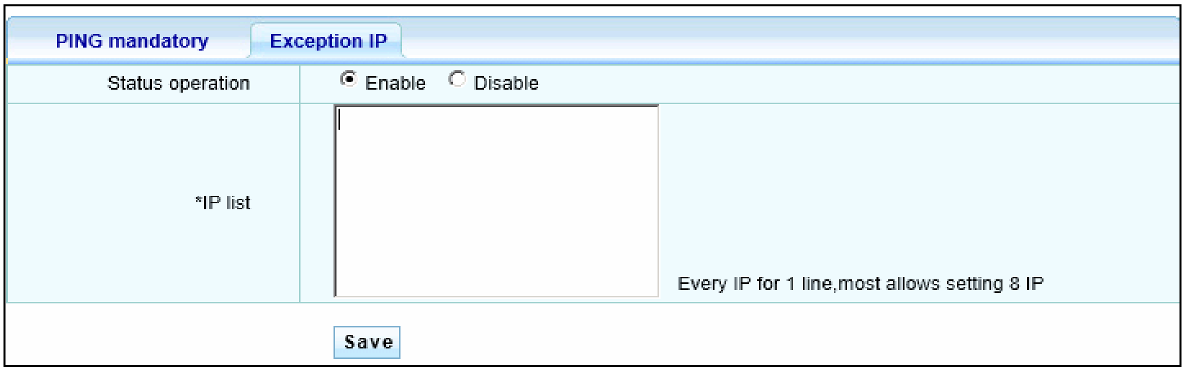
In the configuration page, you can enable and disable PING forced features, enabling viewing PING value in good condition, as shown below:



PING	● Enable ○ Disable

2. Exception IP:

Do not enable PING exception outside the network IP address, as shown below:



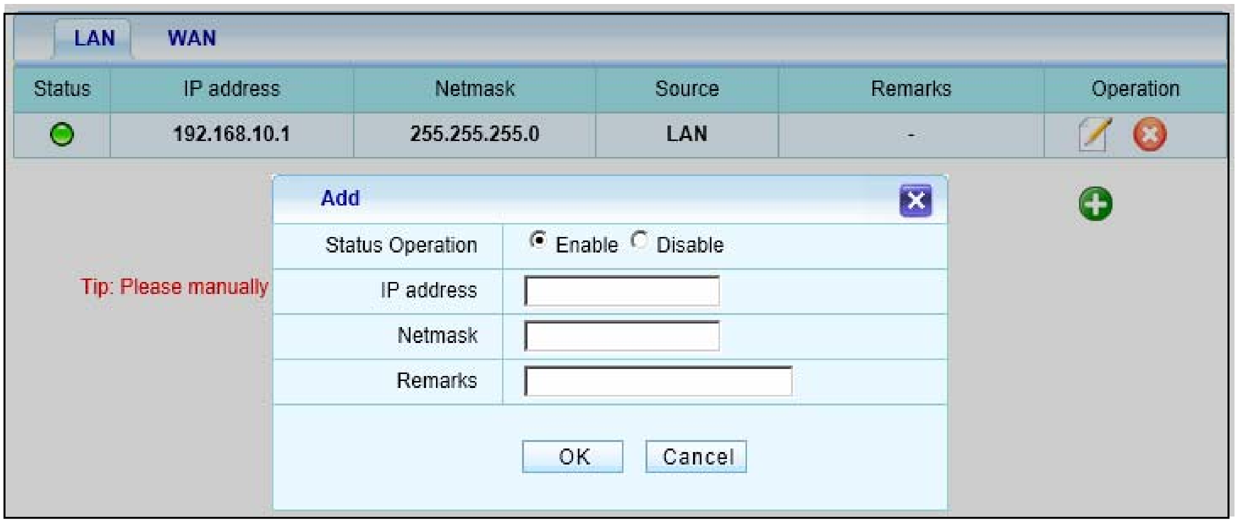
Status operation	● Enable ○ Disable
*IP list	Every IP for 1 line,most allows setting 8 IP

3.8.8 Opening Address

In the configuration page, you can configure this routed intranet or extranet configuration IP addresses, an exception from the firewall operation, normally used in three-layer routing, or outside the network for more than one IP address case.

1. Local area network

LAN domestic demand to open additional IP address, fill in this item, which generally apply in three layer routing case, as shown below:



Status	IP address	Netmask	Source	Remarks	Operation
●	192.168.10.1	255.255.255.0	LAN	-	

Tip: Please manually

Status Operation	● Enable ○ Disable
IP address	
Netmask	
Remarks	

(1) Status operation: Opening address of the enabled or disabled status of this article.

(2) IP address: Enter the IP address.

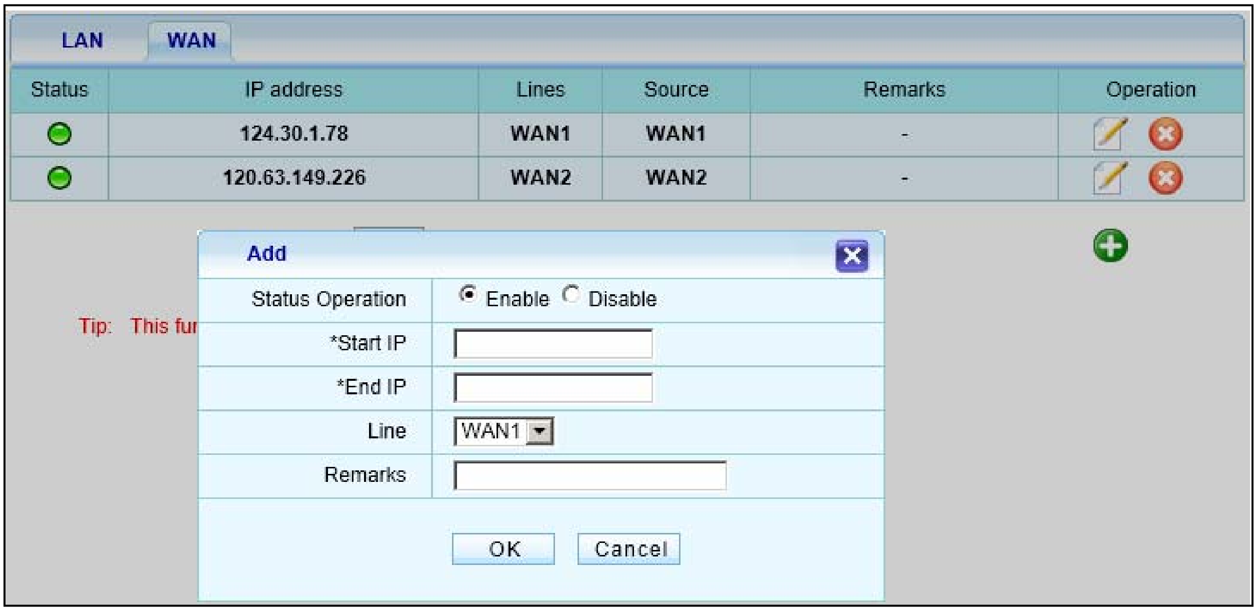
(3) Subnet mask: Routing based on the IP address and subnet mask to calculate to open the IP address range.

(4) Remarks: Explanations for this opening address rules.

(5) Save: Write the static configuration of the router, the parameters to take effect.

2. Wide area network

Wide area network needs an additional open IP address, filled in, as shown below:



Status	IP address	Lines	Source	Remarks	Operation
●	124.30.1.78	WAN1	WAN1	-	
●	120.63.149.226	WAN2	WAN2	-	

Status Operation	● Enable ○ Disable
*Start IP	
*End IP	
Line	WAN1
Remarks	

(1) Status operation: Enable or Disable the operation.

(2) Start IP address: Outside the network you want to open the starting IP address.

(3) End IP address: Open end of the external network IP address.

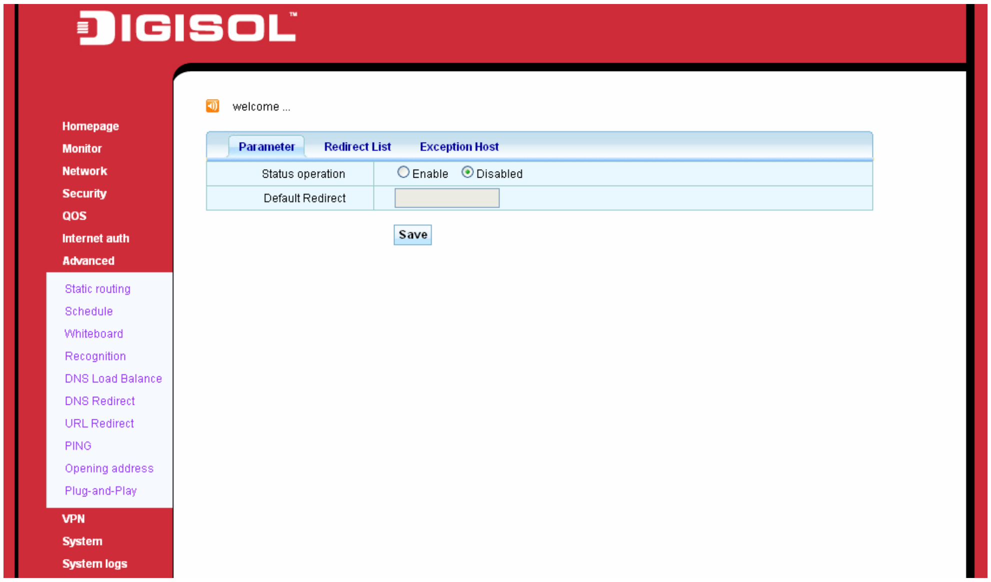
(4) Line: Use this network IP address of WAN lines.

(5) Save: Write the static configuration of the router, the parameters to take effect.

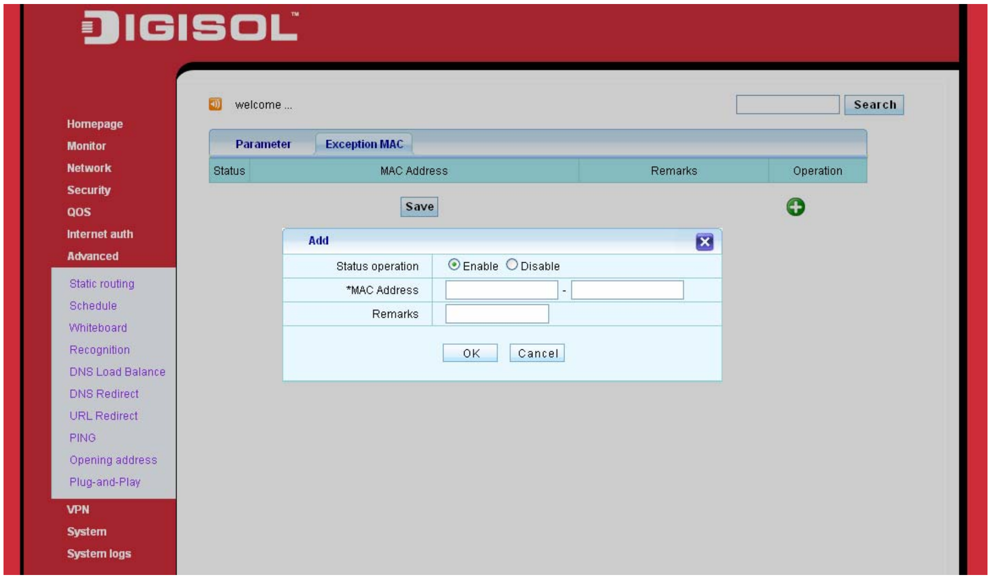
3.8.9 Plug-and-Play

If this feature is enabled, LAN hosts will be unreachable to each other and PPPoE users are not able to access internet.

Add MAC address of a specific user to be exempted from rule list.



Status operation	○ Enable ● Disabled
Default Redirect	



Status	MAC Address	Remarks	Operation

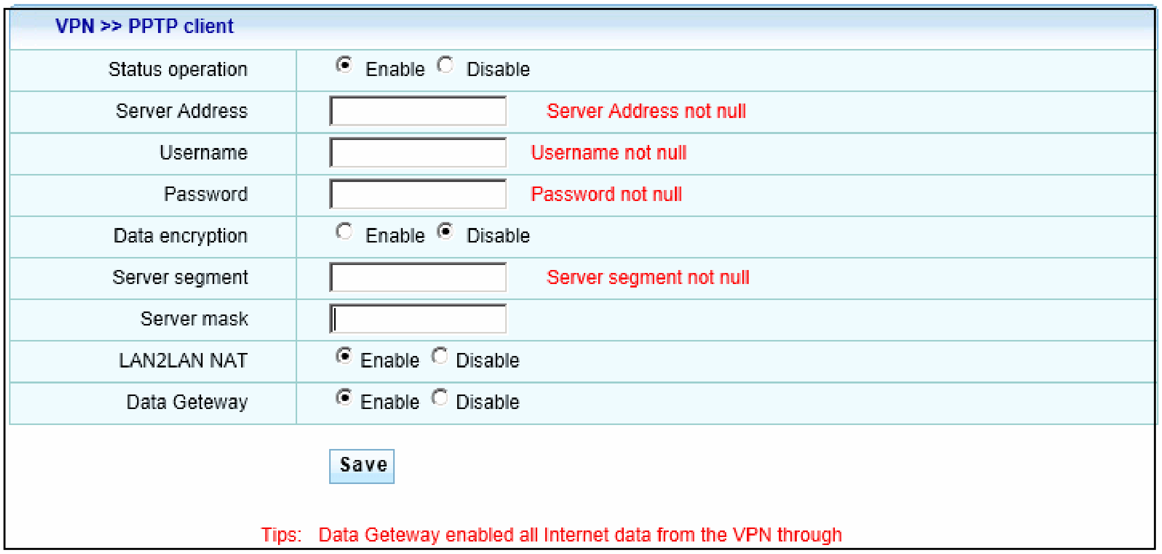
Add

Status operation	● Enable ○ Disable
*MAC Address	-
Remarks	

3.9 VPN Configuration

3.9.1 PPTP client

In this page, you can configure PPTP client and PPTP clients can dial in to the PPTP Server in the routing, as shown below:



VPN >> PPTP client

Status operation	● Enable ○ Disable
Server Address	Server Address not null
Username	Username not null
Password	Password not null
Data encryption	○ Enable ● Disable
Server segment	Server segment not null
Server mask	
LAN2LAN NAT	● Enable ○ Disable
Data Geteway	● Enable ○ Disable

Tips: Data Geteway enabled all Internet data from the VPN through

(1) Status operation: PPTP client Enabled.

(2) Server address: PPTP server outside the network IP address.

(3) Username: Login PPTP Server user name, assigned by the server.

(4) Password: Login PPTP Server password, assigned by the server.

(5)Data encryption: Whether to encrypt the data sent, required service-side remains consistent.

(6) Server segment: PPTP Server IP address.

(7) Server mask: PPTP Server subnet mask.

(8) LAN2LAN NAT: Enable if LAN2LAN NAT is required.

(9) Data Gateway: It will pass internet request via tunnel.

(10) Save: Write the router a static configuration, for the parameters to take effect.

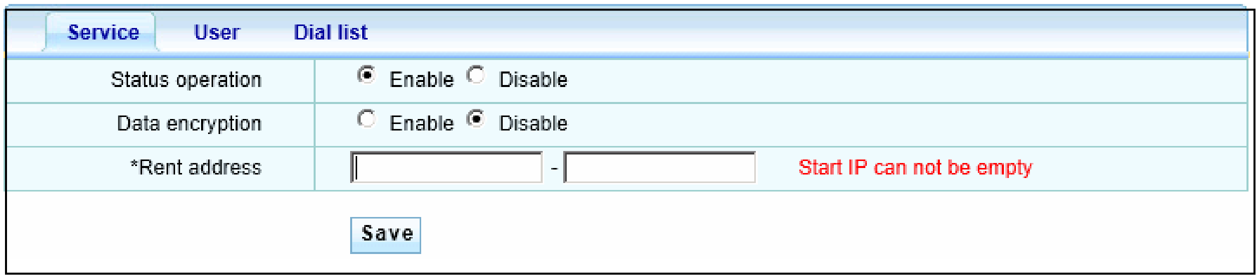
Note: In this page, where "*" must be filled.

3.9.2 PPTP Server

The router supports PPTP VPN that is mainly used for remote users. Use the specified user account through the Internet connection to the corporate network establish a connection, this machine is the same as the one host in the intranet.

Open PPTP Server configuration pages **WEB management interface ->VPN configuration ->PPTP Server**, as shown below:

1. Service configuration



Status operation	● Enable ○ Disable
Data encryption	○ Enable ● Disable
*Rent address	▭ - ▭ Start IP can not be empty

(1) Status operation: Select enable/disable VPN Server.

(2) Data encryption: Select enable/disable to encrypt the transmitted data.

(3) Rent address: Intranet reserved for remote dial-in users IP address. For example: 192.168.1.20-192.168.1.30

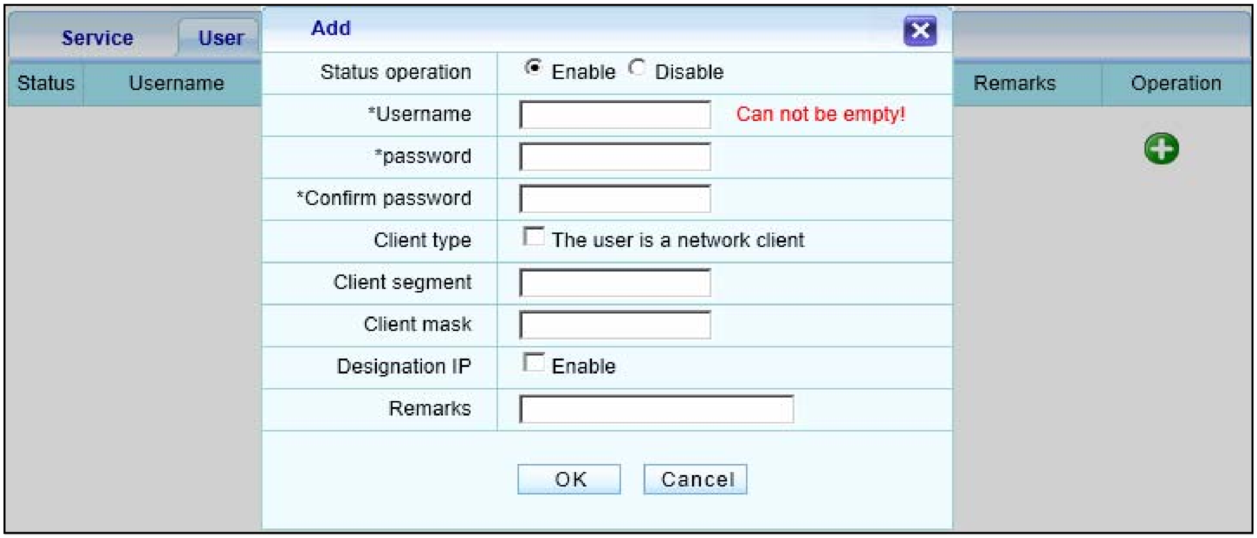
(4) Save: Write the router a static configuration, the parameters to take effect.

2. User management

Create, delete and edit VPN service user account.

(1) Status operation: VPN enabled or disabled status of user.

(2) User name: Create username & Password for PPTP Clients



Status operation	● Enable ○ Disable
*Username	Can not be empty!
*password	
*Confirm password	
Client type	□ The user is a network client
Client segment	
Client mask	
Designation IP	□ Enable
Remarks	

(3) Password: The user's login password.

(4) Confirm password: Confirm password must match the password entered above.

(5) Client type: When dialing VPN Server client to a network (router) when this feature is selected.

(6) Client segments: VPN Clients network address.

(7) Client mask: VPN client by using a subnet mask.

(8) Designation IP: Enter the Fixed IP address for specific user.

(9) Remarks: When there is a need for explanation.

(10) Save: Write the router a static configuration, for the parameters to take effect.

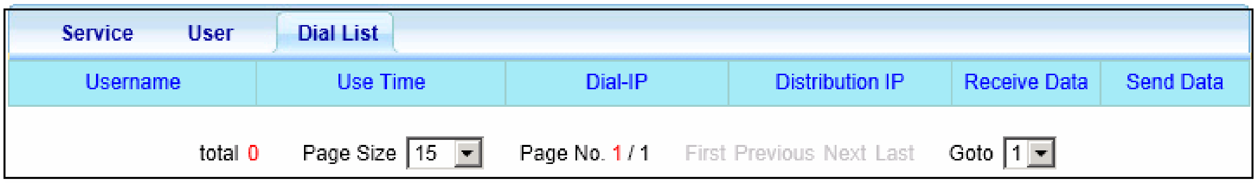
Note:

(1) In this page, after saving configuration changes and, with immediate effect.

(2) Password and confirm password must be entered.

3. Dial list

In this page, you can view the dial-in to these routing VPN users, as shown below:



Username	Use Time	Dial-IP	Distribution IP	Receive Data	Send Data

total 0 Page Size 15 Page No. 1 / 1 First Previous Next Last Goto 1

(1) User name: Dial-in to this routing VPN user name of the user, assigned by the route.

(2) Use Time: Active user time.

(3) Dial IP: Dial-in to this routing VPN users outside the network IP address.

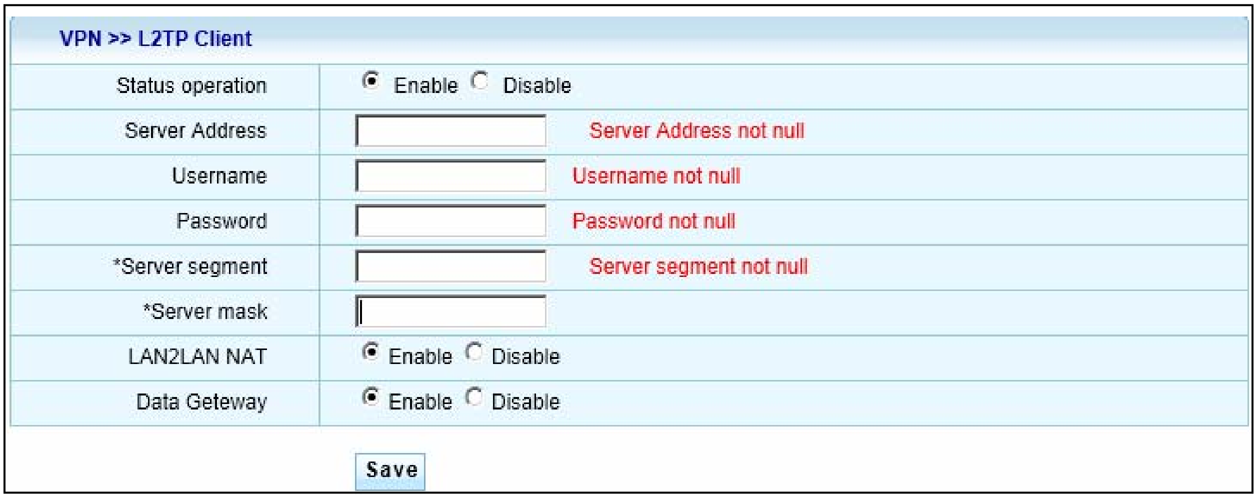
(4) Distribution IP: Route to the VPN IP address.

(5) Receive Data: Data Received

(6) Send Data: Data sent.

3.9.3 L2TP Client

In this page, you can configure L2TP client and L2TP clients can dial in to the PPTP Server in the routing, as shown below.


VPN >> L2TP Client

Status operation	● Enable ○ Disable
Server Address	Server Address not null
Username	Username not null
Password	Password not null
*Server segment	Server segment not null
*Server mask	
LAN2LAN NAT	● Enable ○ Disable
Data Geteway	● Enable ○ Disable

(1) Status operation: L2TP client restart disabled.
(2) Server address: L2TP server outside the network IP address.

(3) Username: Login L2TP Server user name, assigned by the server.

(4) Password: Login L2TP Server password, assigned by the server.

(5) L2TP Server segment: L2TP Server IP address.

(6) L2TP Server mask: L2TP Server subnet mask.

(7) LAN2LAN NAT: Enable if LAN2LAN NAT is required

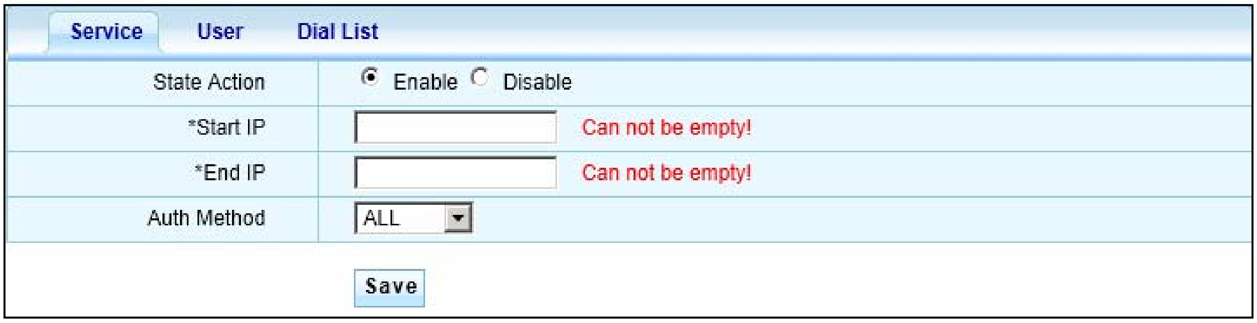
(8) Data Gateway: It will pass internet request via tunnel.

(9) Save: Write the router a static configuration, for the parameters to take effect.

3.9.4 L2TP Server

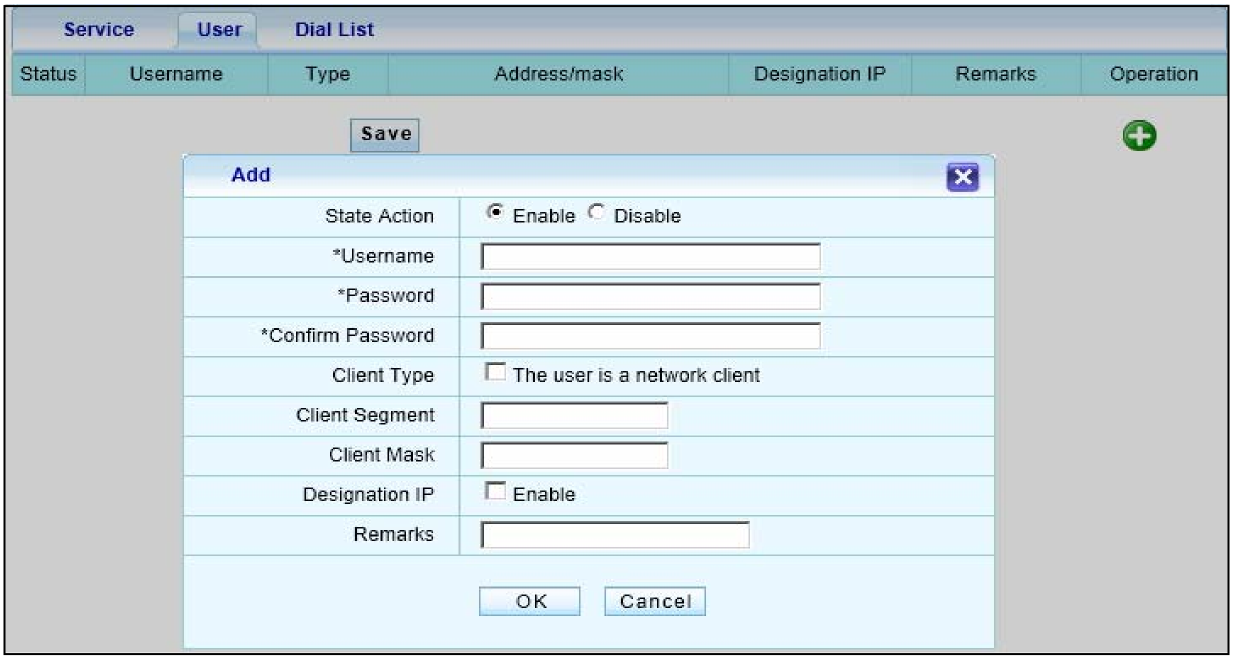
The router supports L2TP VPN that is mainly used for remote users. Use the specified user account through the Internet connection to the corporate network to establish a connection, this machine is the same as the one host in the intranet.

Open L2TP Server configuration pages **WEB management interface ->VPN configuration ->L2TP Server**, as shown below:



State Action	● Enable ○ Disable
*Start IP	Can not be empty!
*End IP	Can not be empty!
Auth Method	ALL

2. User management



Status	Username	Type	Address/mask	Designation IP	Remarks	Operation

State Action	● Enable ○ Disable
*Username	
*Password	
*Confirm Password	
Client Type	□ The user is a network client
Client Segment	
Client Mask	
Designation IP	□ Enable
Remarks	

Create, delete and edit VPN service user account.

(1) State action: VPN enabled or disabled status of user.

(2) User name: Create username & Password for L2TP Clients

(3) Password: The user's login password.

(4) Confirm password: Confirm password must match the password entered above.

(5) Client type: When dialing VPN Server client to a network (router) when this feature is selected.

(6) Client segments: VPN Clients network address.

(7) Client mask: VPN client by using a subnet mask.

(8) Destination IP: Enter the Fixed IP address for specific user.

(9) Note: When there is a need for explanation.

(10) Save: Write the router a static configuration, for the parameters to take effect.

Note:

(1) In this page, after saving configuration changes and, with immediate effect.

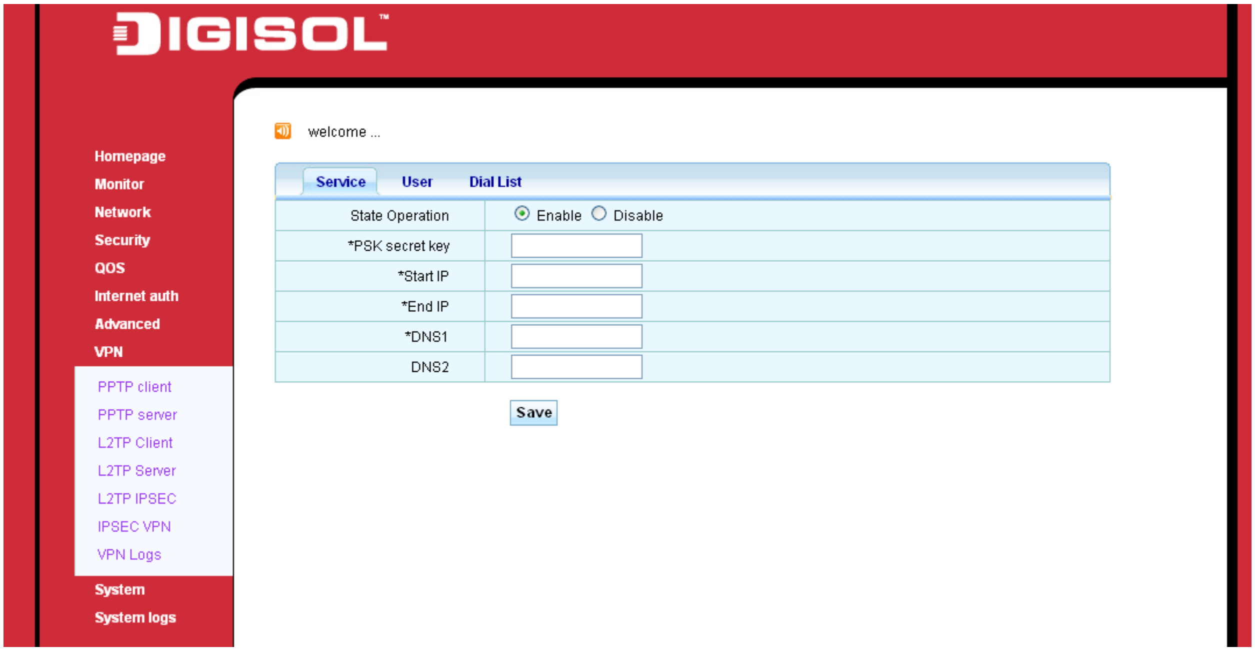
(2) Password and confirm password must be entered

3.9.5 L2TP IPSec

L2TP over IPSec VPNs enable a business to transport data over the Internet, while still maintaining a high level of security to protect data. You can use this type of secure connection for small or remote office clients that need access to the corporate network. You can also use L2TP over IPSec VPNs for routers at remote sites by using the local ISP and creating a demand-dial connection into corporate headquarters.

Define following parameter for creating L2TP IPSec Server:

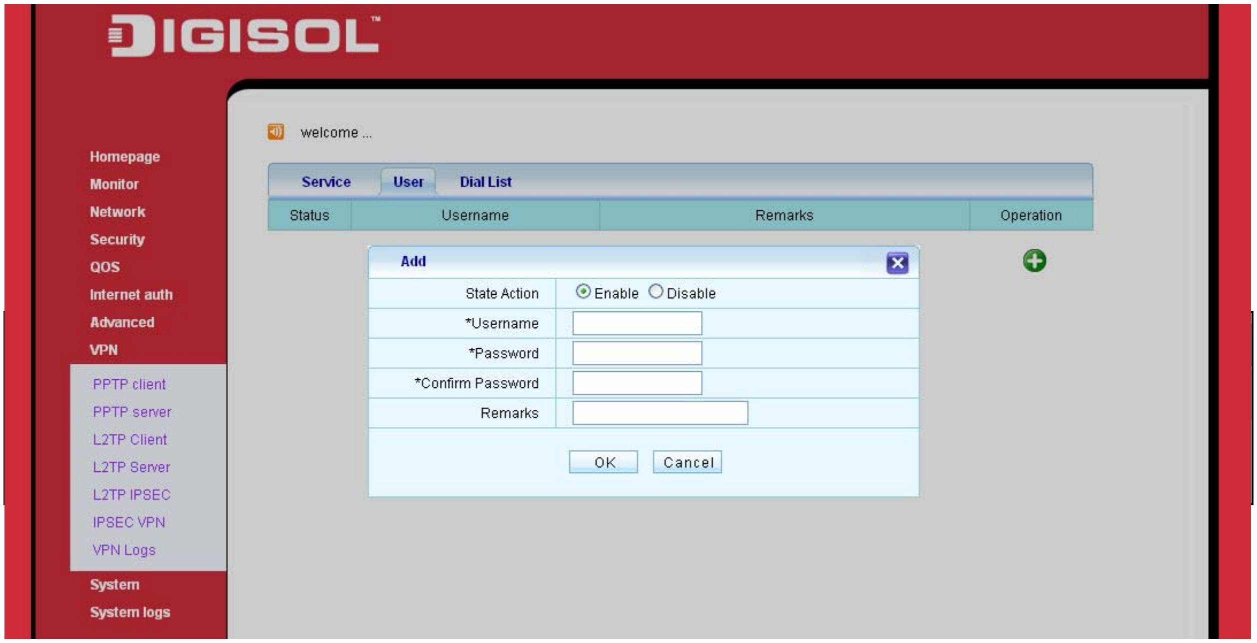
1. State Operation: Enable/Disable
2. PSK secret key: Define the key string here. User will use this key for remote dial-in.
3. Start IP: Start IP address for uses.
4. End IP: End IP address for uses.
5. DNS1: DNS for users.
6. DNS2: DNS for users.



State Operation	● Enable ○ Disable
*PSK secret key	
*Start IP	
*End IP	
*DNS1	
DNS2	

Define following parameters for creating users:

7. State Action: Enable/Disable
8. Username
9. Password
10. Confirm Password



State Action ● Enable ○ Disable

*Username

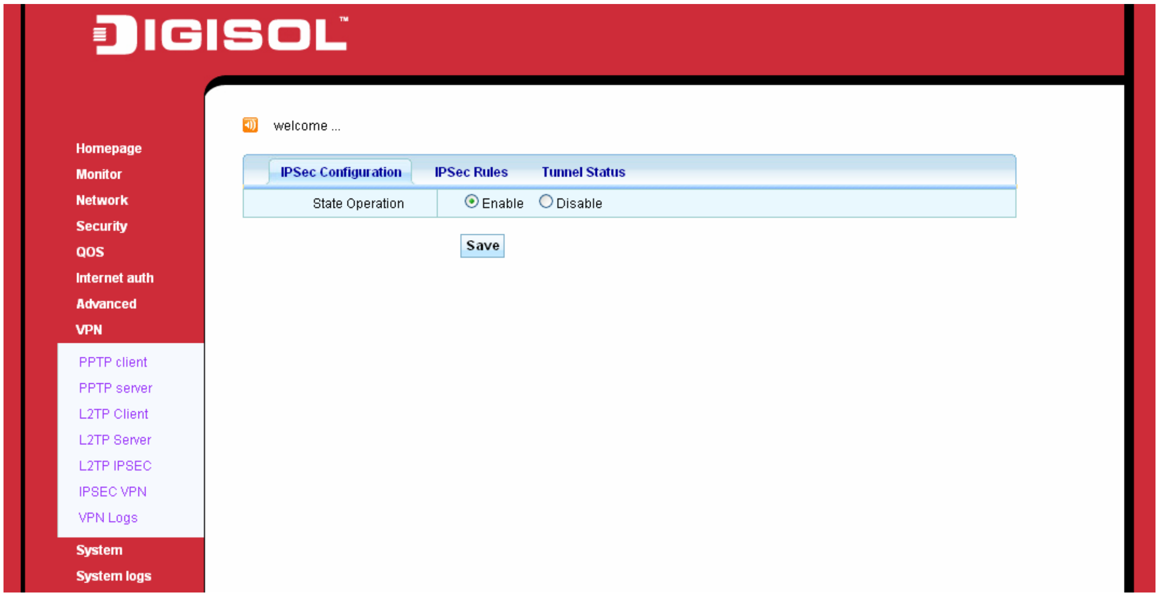
*Password

*Confirm Password

Remarks

3.9.6 IPSec VPN

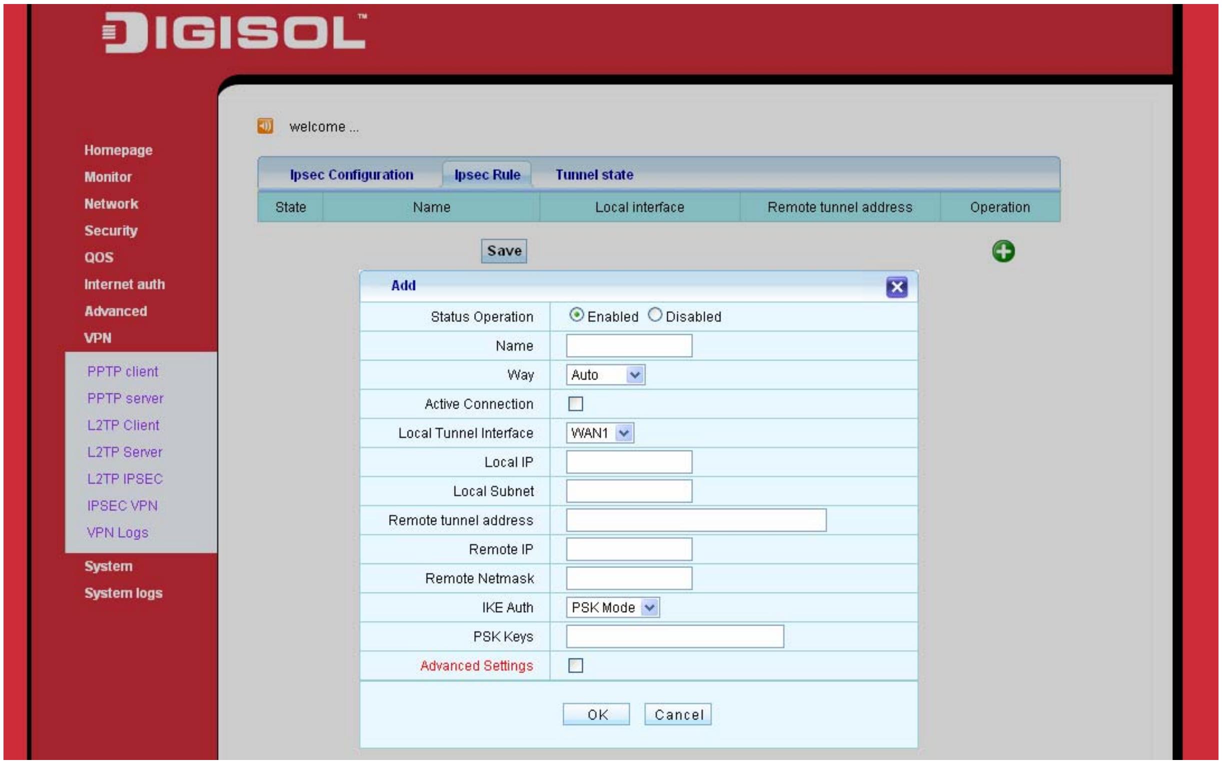
Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session.



State Operation ● Enable ○ Disable

Define following parameters IPSEC Tunnel

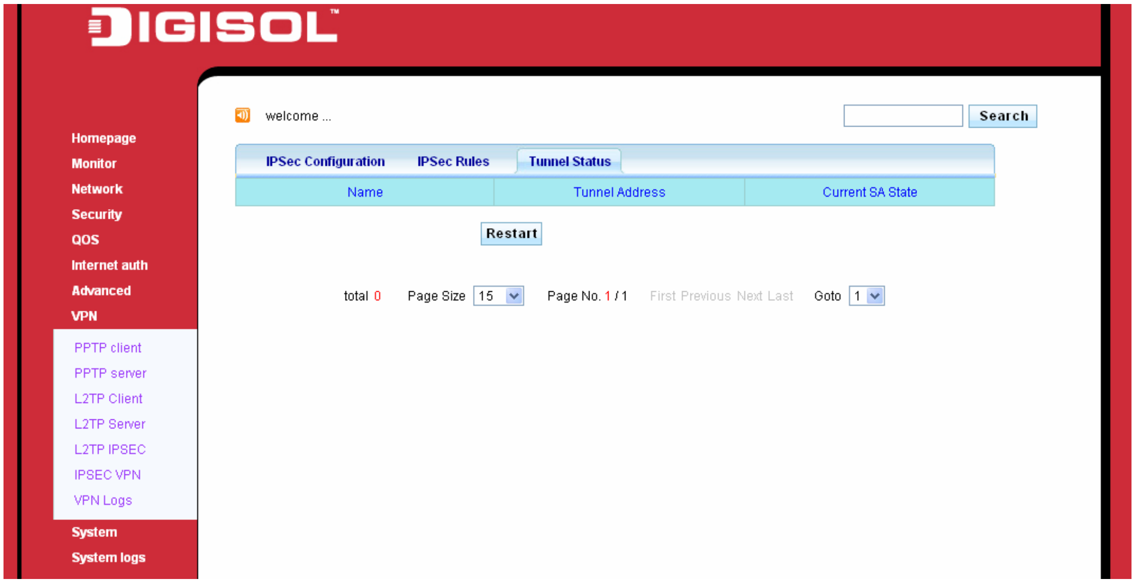
1. Status Operation: Enabled/Disabled
2. Name: Identification name for Tunnel Interface
3. Way: Auto/Custom.
4. Active Connection: Use this tunnel as either active or standby.
5. Local Tunnel Interface: WAN1/WAN2
6. Local IP: Define Local LAN ip address
7. Local Subnet: Define Local LAN subnet information.
8. Remote tunnel address: Define WAN IP address of remote router
9. Remote IP: Define LAN network of remote device
10. Remote Netmask: Define Remote LAN subnet mask
11. IKE Auth: PSK Mode
12. PSK Keys: Enter pass key. Key should match at both the ends.
13. Advanced Settings: Define IKE and IPSEC proposal settings. This setting must match on both local and remote router.



State	Name	Local interface	Remote tunnel address	Operation

Status Operation	● Enabled ○ Disabled
Name	
Way	Auto
Active Connection	□
Local Tunnel Interface	WAN1
Local IP	
Local Subnet	
Remote tunnel address	
Remote IP	
Remote Netmask	
IKE Auth	PSK Mode
PSK Keys	
Advanced Settings	□

Tunnel status will display the status of the configured tunnel. Tunnel state will be UP (active) if both routers negotiate all the defined parameters successfully.

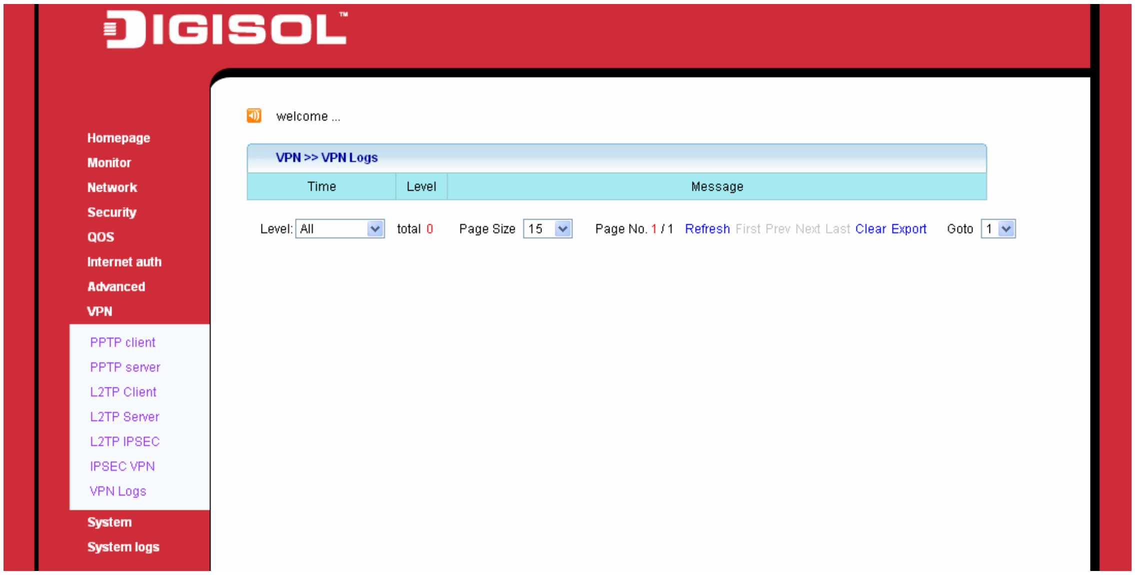


Name	Tunnel Address	Current SA State

total 0 Page Size 15 Page No. 1 / 1 Goto 1

3.9.7 VPN Logs

All log messages related to Tunnel negotiation are displayed on this page.



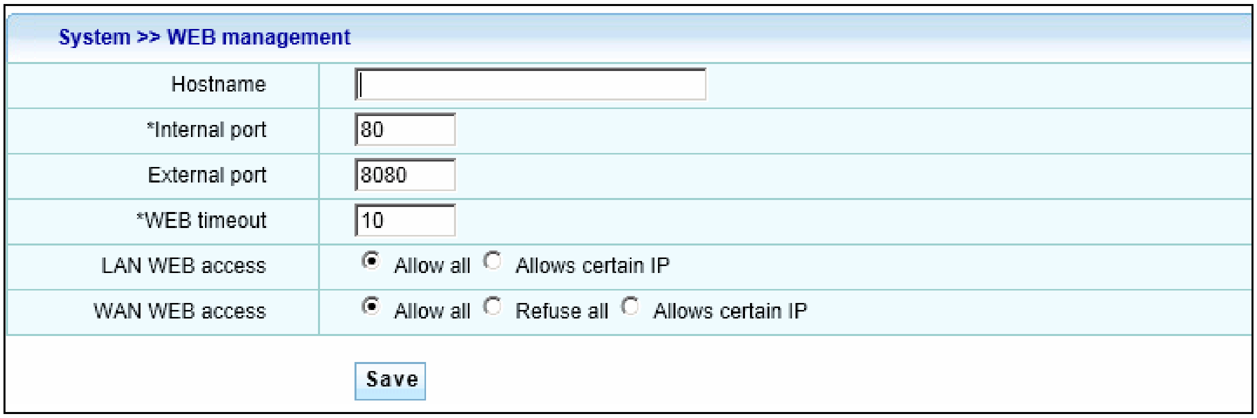
Time	Level	Message

Level: All total 0 Page Size 15 Page No. 1 / 1 Goto 1

3.10 System

3.10.1 WEB Management settings

Open the basic settings page **WEB management interface->System settings->WEB Management**, as shown below:



System >> WEB management

Hostname	
*Internal port	80
External port	8080
*WEB timeout	10
LAN WEB access	● Allow all ○ Allows certain IP
WAN WEB access	● Allow all ○ Refuse all ○ Allows certain IP

(1) Host name: Name of the router.

(2) WEB intranet port: Intranet login to the router using the WEB management port.

(3) WEB network port: Extranet login to the router using the WEB management port.

(4) WEB time out: WEB communication timeout.

(5) Intranet WEB permissions: To router WEB Management internal host range.

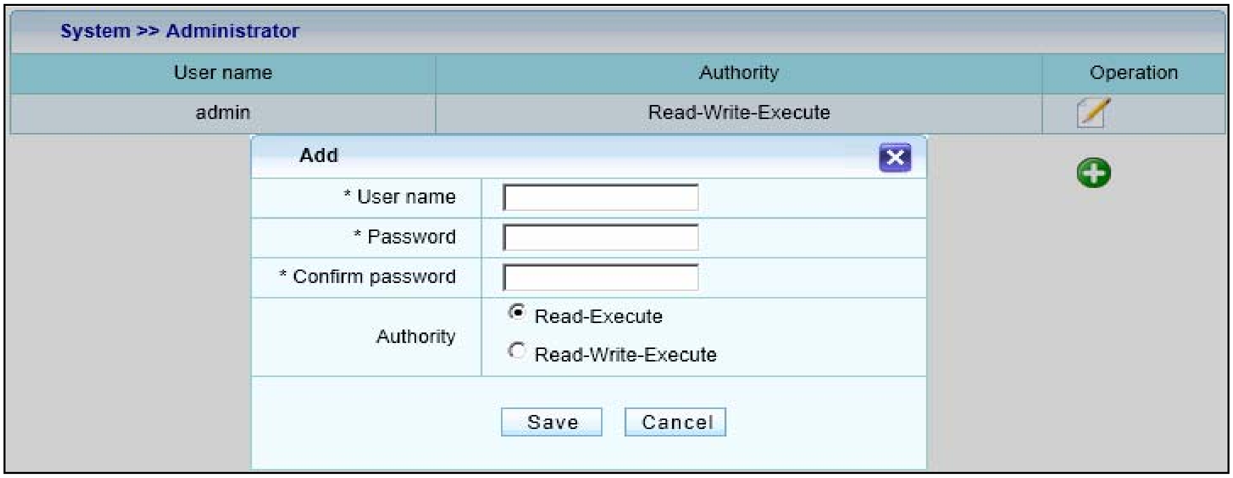
(6) Outside the network WEB permissions: To router WEB management of external host range.

(7) Save: Write the static configuration of the router, for the parameters to take effect.

3.10.2 Administrator settings

In this page, you can set login WEB Management page of the user's user name, password, and managing permissions.

Open the Administrator's configuration page **WEB management interface->System-> Administrator**, as shown below:



System >> Administrator

User name	Authority	Operation
admin	Read-Write-Execute	

Add

* User name	
* Password	
* Confirm password	
Authority	● Read-Execute ○ Read-Write-Execute

(1) User name: The user name of the user logged on to the system.

(2) Password: The user's login password.

(3) Confirm password: Confirm password must match the password entered above.

(4) Permissions: Users have the right to operation of the system.

Note: (1) With " *" Identity is required.

(2) New password and confirm password values must be consistent values.

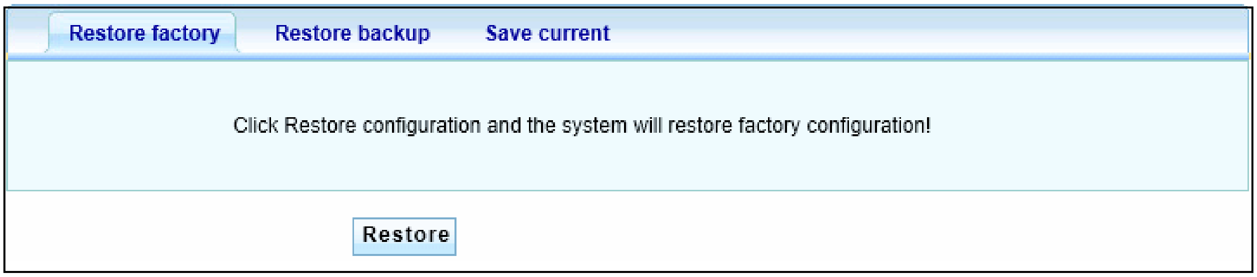
(3) Password to modify and then keep, if you lose the password, you will not be able to login to the router, you must restore the router to factory settings.

3.10.3 Profile

1. Restore Factory

In the configuration page, you can configure router restore factory operations.

Open the restore factory settings page **WEB management interface->System->Administrator ->Restore factory settings**, as shown below:



Click Restore configuration and the system will restore factory configuration!

Restore: Click to restore factory configuration operation.

Note:

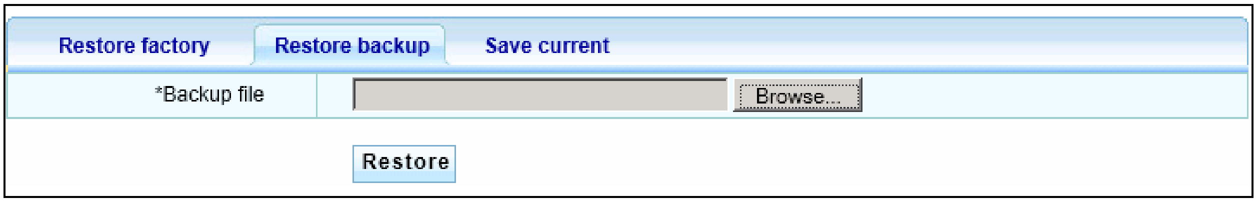
(1) In the configuration page, after restoring factory configuration was successful, the system will automatically restart.

(2) After the system starts successfully, you can use http://192.168.0.1 access router WEB Config page.

2. Restore backup

In the configuration page, you can restore the previously saved configuration of the router.

Open the restore backup settings page **WEB management interface -> System->Administrator -> Restoring backup**, as shown below:



*Backup file

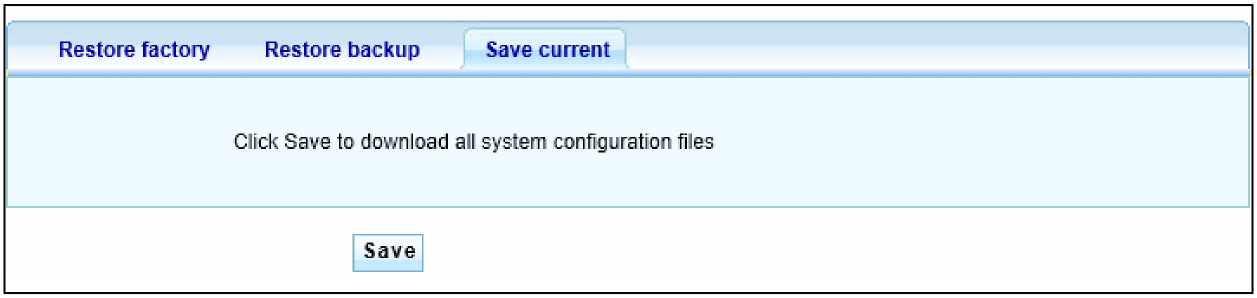
Backup file: Saves the backup configuration files.

Note: After you recover the backup configuration was successful, the system will automatically restart.

3. Save the current

In the configuration page, you can save the current configuration of the router.

Opens the Save current configuration page **WEB management interface -> System Setup ->Administrator ->Save current**, as shown below:



Click Save to download all system configuration files

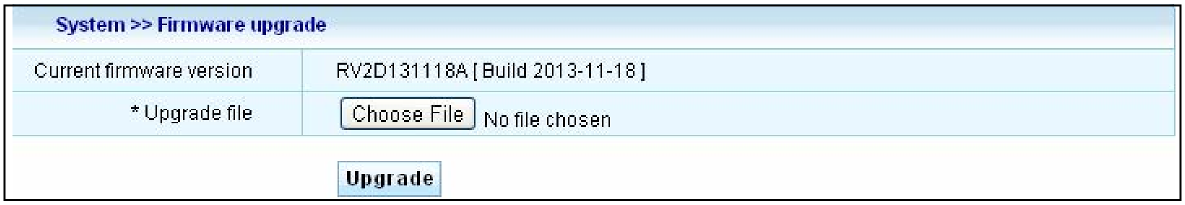
Save configuration: Back up the current configuration of the router.

Note: Click the "save configuration" button, downloading system the current configuration file.

3.10.4 Firmware upgrade

Firmware upgrade of the products is an indispensable feature of the network, network application environment changes rapidly, must continually through the optimization and upgrading of software to suit different application needs. Can the needs change quickly launch the software upgrade, more and more user attention.

Open firmware upgrade configuration pages **WEB management interface ->System-> Firmware upgrade**, as shown below:



Current firmware version	RV2D131118A [Build 2013-11-18]
* Upgrade file	Choose File No file chosen

Current firmware version: Displays the version number of the software used by the current system.

The upgrade file: You want to use to upgrade your system software package, supplied by the manufacturer.

Note:

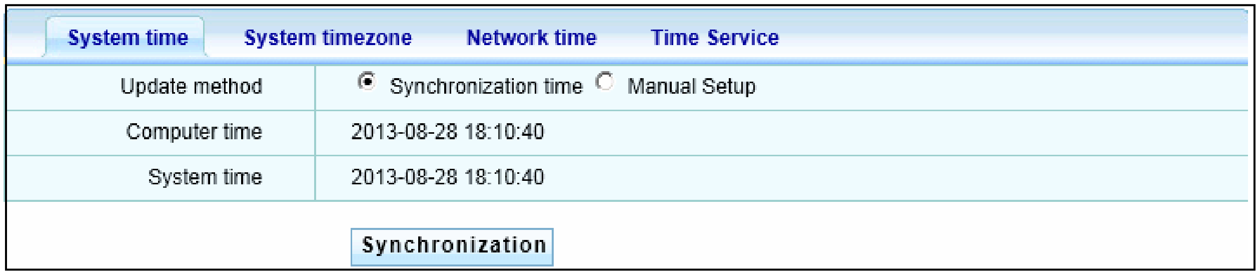
(1) "*" identity is mandatory field

(2) Firmware upgrade once started do not terminate, the whole upgrade process needs 3-5 minutes. After successful initializing upgrade process the system prompts, please be patient during the period.

(3) After the upgrade is successful, the system will prompt for restart to get the new firmware in effect so that the new version is valid. If Upgrade error is prompted, do not repeat the upgrade until restart router prompt the upgrade is successful. If you upgrade an error and has accidentally shutdown or power failure during the upgrade, system will not start is the case, please contact a factory technician to solve your problem in a timely manner.

3.10.5 System Time

1) System Time
The time settings page. You can set the router time.
Open the system configuration page **WEB management interface -> System Setup ->System Time.**



Update method	● Synchronization time ○ Manual Setup
Computer time	2013-08-28 18:10:40
System time	2013-08-28 18:10:40

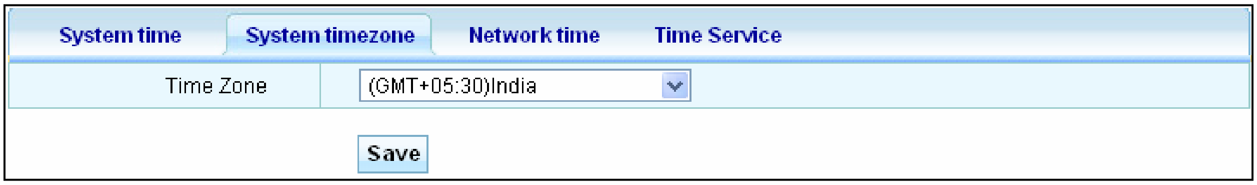
(1) Update method: Modified the way, into two kinds: synchronize computer time and manually set up.

(2) Computer time: Synchronized with the computer time.

(3) System time: the time display to open the router setup page.

2. System Timezone

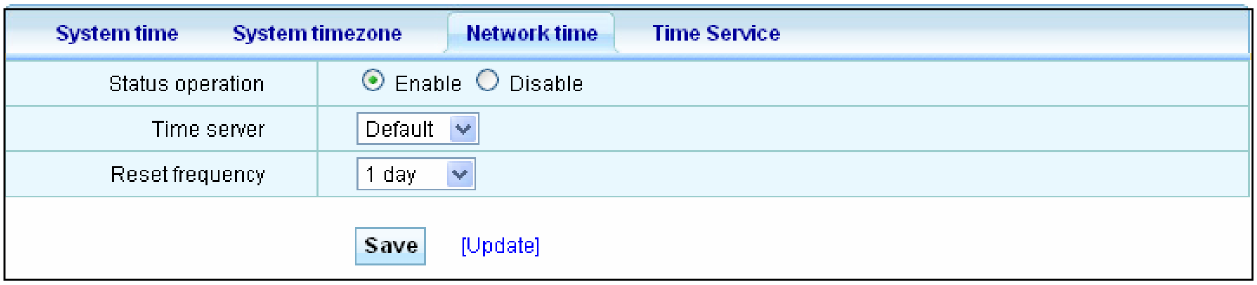
Select the timezone parameter as per the County settings. For India, select from drop-down list as (GMT+5.30) India and save settings.



Time Zone: (GMT+05:30)India

3. Network Time

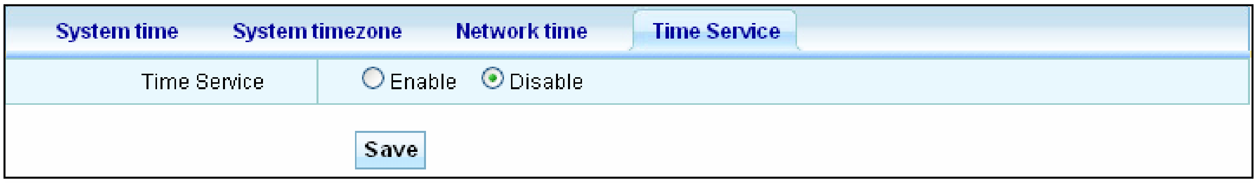
Auto detect or manually define the IP address of NTP server for time synchronization.



Status operation: ● Enable ○ Disable
Time server: Default
Reset frequency: 1 day

4. Time Service

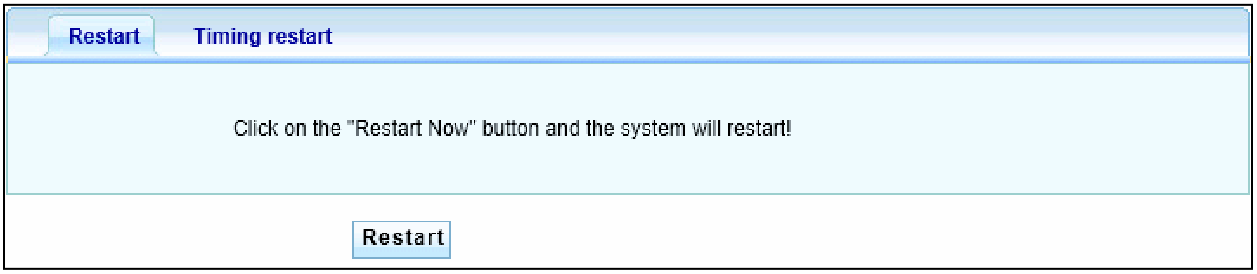
Enable/Disable time service.



Time Service: ○ Enable ● Disable

3.10.6 Restart

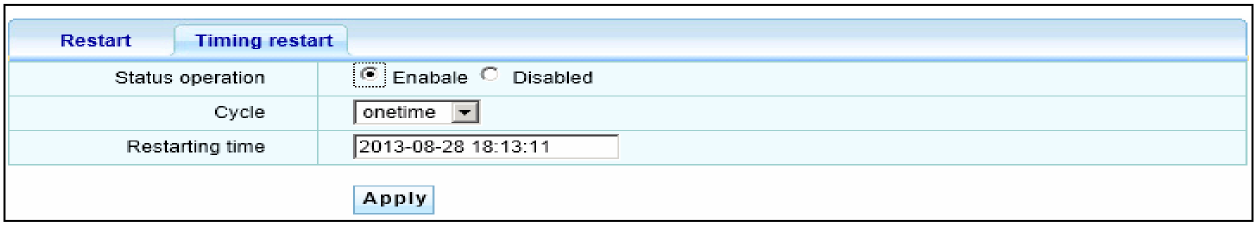
In the configuration page, you can reset the router operations.
Restart the configuration page, open **WEB management interface ->System->Restart**, as shown:



Click on the "Restart Now" button and the system will restart!

Restart: Select this button; click "**apply**", the router will restart now.

Timed cycle: To the routing set an automatic restart of the time.



Status operation	● Enabale ○ Disabled
Cycle	onetime
Restarting time	2013-08-28 18:13:11

Status operation: Enable or disable a scheduled restart capabilities.

Cycle: Scheduled reboot cycle.

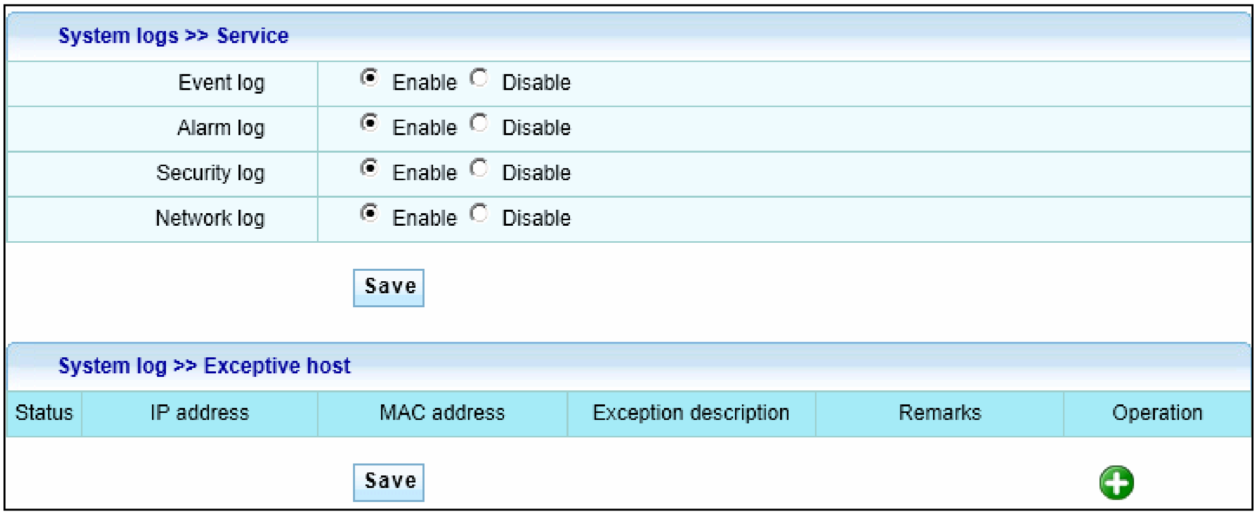
Restart time: Set a restart time, while the system is running at this time, it will automatically restart.

3.11 System logs

Record router running profile, save the logging information to help us for fault location, troubleshooting and network security management, Can help us analyze the device is working correctly, network health.

3.11.1 Service configuration

Opens the service configuration page **WEB management interface->System logs->Service**, as shown below:



System logs >> Service

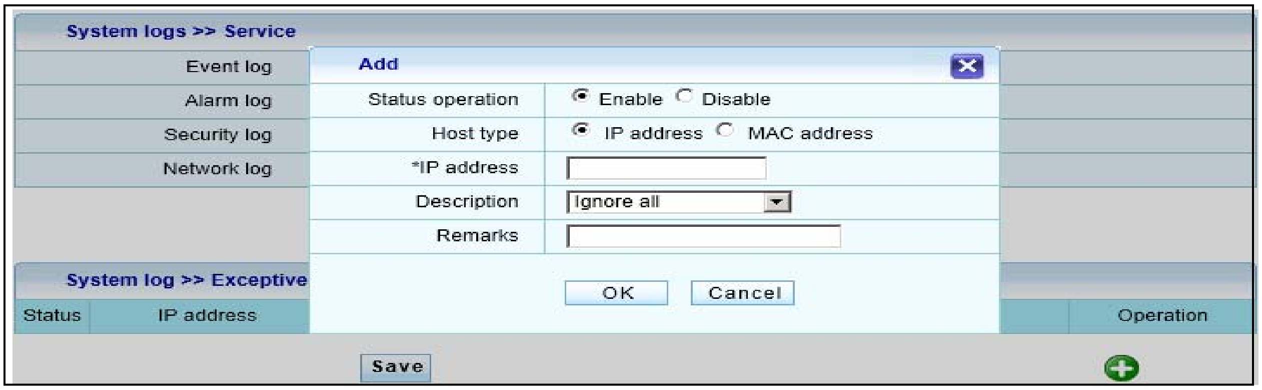
Event log	● Enable ○ Disable
Alarm log	● Enable ○ Disable
Security log	● Enable ○ Disable
Network log	● Enable ○ Disable

System log >> Exceptive host

Status	IP address	MAC address	Exception description	Remarks	Operation

3.11.2 Exceptional hosts

Opens the log configuration page **WEB management interface -> System logs-> exceptional hosts**, as shown:



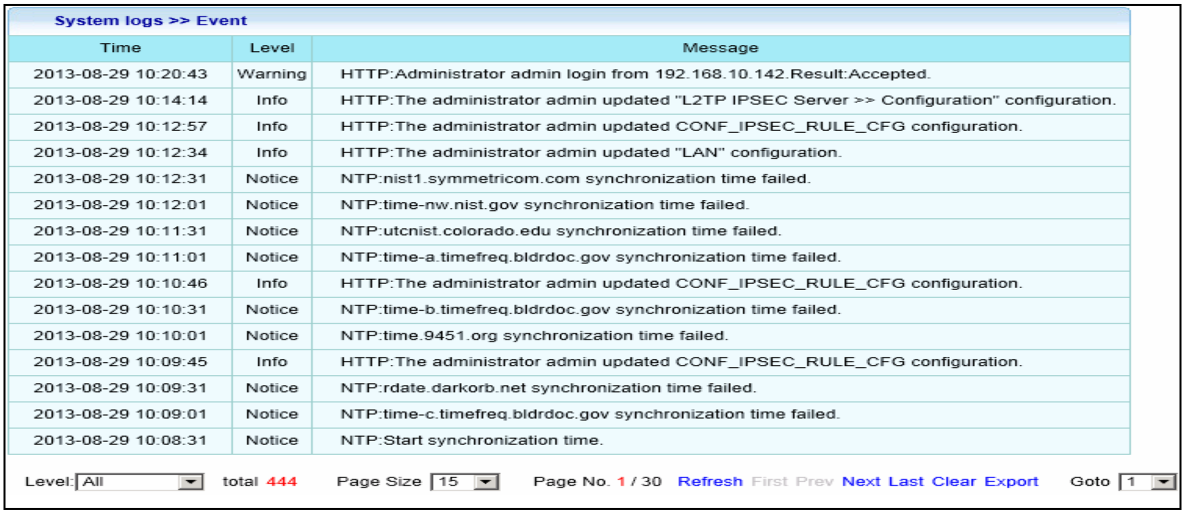
Add

Status operation	● Enable ○ Disable
Host type	● IP address ○ MAC address
*IP address	
Description	Ignore all
Remarks	

(1) IP addresses: Sets the exception of host IP addresses.
(2) Exception description: Set log contents are ignored by this exceptional host.

3.11.3 The event log

Opens the log configuration page **WEB management interface ->System logs->Event**, as shown below:


System logs >> Event

Time	Level	Message
2013-08-29 10:20:43	Warning	HTTP:Administrator admin login from 192.168.10.142.Result:Accepted.
2013-08-29 10:14:14	Info	HTTP:The administrator admin updated "L2TP IPSEC Server >> Configuration" configuration.
2013-08-29 10:12:57	Info	HTTP:The administrator admin updated CONF_IPSEC_RULE_CFG configuration.
2013-08-29 10:12:34	Info	HTTP:The administrator admin updated "LAN" configuration.
2013-08-29 10:12:31	Notice	NTP:nist1.symmetricom.com synchronization time failed.
2013-08-29 10:12:01	Notice	NTP:time-nw.nist.gov synchronization time failed.
2013-08-29 10:11:31	Notice	NTP:utcnist.colorado.edu synchronization time failed.
2013-08-29 10:11:01	Notice	NTP:time-a.timefreq.bldrdoc.gov synchronization time failed.
2013-08-29 10:10:46	Info	HTTP:The administrator admin updated CONF_IPSEC_RULE_CFG configuration.
2013-08-29 10:10:31	Notice	NTP:time-b.timefreq.bldrdoc.gov synchronization time failed.
2013-08-29 10:10:01	Notice	NTP:time.9451.org synchronization time failed.
2013-08-29 10:09:45	Info	HTTP:The administrator admin updated CONF_IPSEC_RULE_CFG configuration.
2013-08-29 10:09:31	Notice	NTP:rdate.darkorb.net synchronization time failed.
2013-08-29 10:09:01	Notice	NTP:time-c.timefreq.bldrdoc.gov synchronization time failed.
2013-08-29 10:08:31	Notice	NTP:Start synchronization time.

Level: All total 444 Page Size 15 Page No. 1 / 30 Refresh First Prev Next Last Clear Export Goto 1

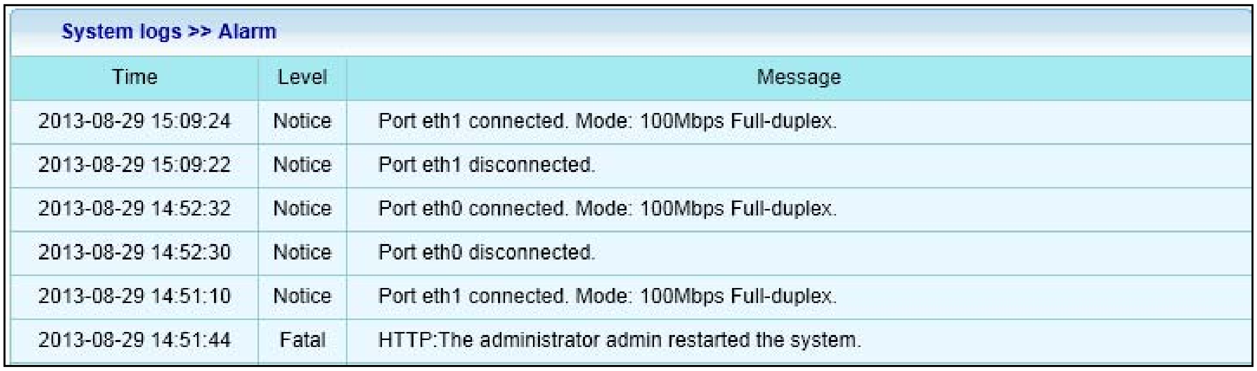
(1) Time: Instant time system status change occurs.

(2) Level: Is divided into information and warnings. "Information" is a record runs of events, the "warning" record run events on the basis of the alerts.

(3) Message: Record run of events.

3.11.4 Alarm log

Open the alarm log configuration page **WEB management interface->System logs->Alarm**



System logs >> Alarm

Time	Level	Message
2013-08-29 15:09:24	Notice	Port eth1 connected. Mode: 100Mbps Full-duplex.
2013-08-29 15:09:22	Notice	Port eth1 disconnected.
2013-08-29 14:52:32	Notice	Port eth0 connected. Mode: 100Mbps Full-duplex.
2013-08-29 14:52:30	Notice	Port eth0 disconnected.
2013-08-29 14:51:10	Notice	Port eth1 connected. Mode: 100Mbps Full-duplex.
2013-08-29 14:51:44	Fatal	HTTP:The administrator admin restarted the system.

(1) Time: Instant time system status change occurs.

(2) Level: warning. "Warning" reminds you to get attention.

(3) Message: Record run of events.

(4) Refresh: Click the "Refresh" button can be brushed into the most recent log information.

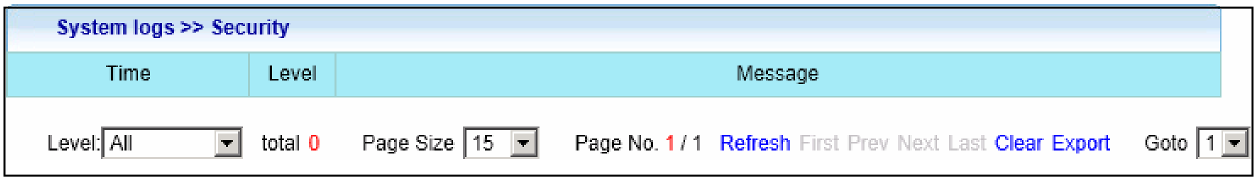
(5) Remove: Click the "clear" button you can clear the log information.

(6) Export: Click "export" button to export the log to a Notepad.

3.11.5 The security log

This log tracks events such as logon, change access permissions and system startup and shutdown.

Open the security log configuration page **WEB management interface->System logs-> Security**, as shown below:



System logs >> Security

Time	Level	Message

Level: All ▾ total 0 Page Size 15 ▾ Page No. 1 / 1 Refresh First Prev Next Last Clear Export Goto 1 ▾

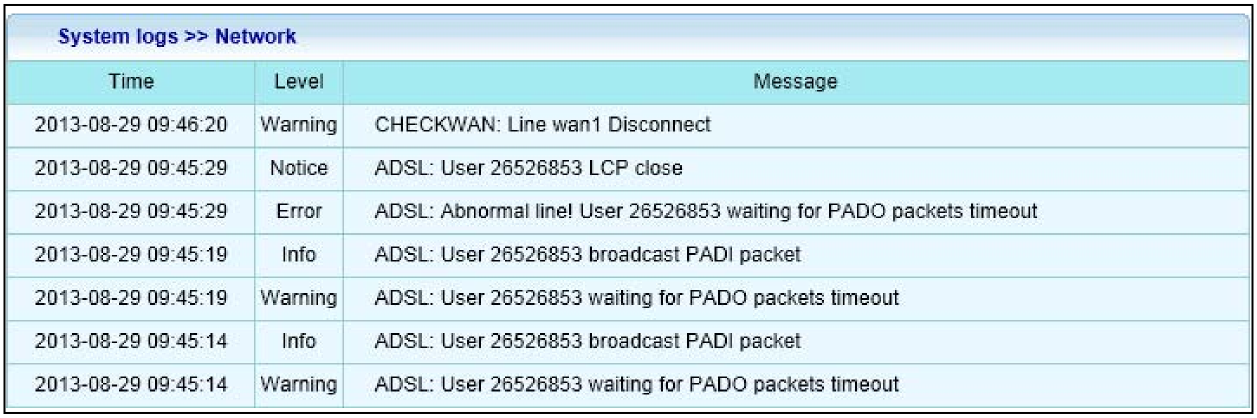
(1) Time: Instant time system status change occurs.

(2) Level: Is divided into information and warnings. "**Information**" is a record run of events, “**warning**" is record run events on the basis of the alert.

(3) Message: Record run of events.

3.11.6 Log

Open the network configuration page **WEB management interface->System logs->Network** , as shown below:



System logs >> Network

Time	Level	Message
2013-08-29 09:46:20	Warning	CHECKWAN: Line wan1 Disconnect
2013-08-29 09:45:29	Notice	ADSL: User 26526853 LCP close
2013-08-29 09:45:29	Error	ADSL: Abnormal line! User 26526853 waiting for PADO packets timeout
2013-08-29 09:45:19	Info	ADSL: User 26526853 broadcast PADI packet
2013-08-29 09:45:19	Warning	ADSL: User 26526853 waiting for PADO packets timeout
2013-08-29 09:45:14	Info	ADSL: User 26526853 broadcast PADI packet
2013-08-29 09:45:14	Warning	ADSL: User 26526853 waiting for PADO packets timeout

(1) Time: Instant time system status change occurs.

(2) Level: Is divided into information and warnings. "**Information**" is a record run of events, the "**warning**" record run events on the basis of the alert.

(3) Message: Record run of events.

(4) Refresh: Click the "**Refresh**" button can be brushed into the most recent log information.

(5) Remove: Click the "**clear**" button you can clear the log information.

(6) Export: Click "**export**" button to export the log to a Notepad.

4. Appendix

Hardware recovery configuration

If router password loss or other reasons, you need to configure the router back to its factory configuration when, through the device front panel RST/CLR button configuration empty.

Action steps:

Step 1: To power up the router, start the routing to a functional State (SYS light flashes regularly).

Step 2: Use a pointed object, press and hold the front panel RST button down, wait about 3 seconds, release the RST button (Based on the routing type and versions, may be different)

Step 3: The router automatically restarts and restores system to factory default condition.

Note: (1) This feature requires a routing boots can take effect only after (SYS light flashes regularly).

(2) RST button must have to hold, not midway released (according to the routing type and versions, may be different).